2017

E-INVIGILATION OF E-ASSESSMENTS

Ketab, Salam

E-INVIGILATION OF E-ASSESSMENTS

By

SALAM KETAB

B.Sc., M.Sc.

A thesis submitted to Plymouth University in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

Faculty of Science and Engineering

July 2017

COPYRIGHT STATEMENT

Abstract

E-learning and particularly distance-based learning is becoming an increasingly important mechanism for education. A leading Virtual Learning Environment (VLE) reports a user base of 70 million students and 1.2 million teachers across 7.5 million courses. Whilst e-learning has introduced flexibility and remote/distance-based learning, there are still aspects of course delivery that rely upon traditional approaches. The most significant of these is examinations. The lack of being able to provide invigilation in a remote-mode has restricted the types of assessments, with exams or in-class test assessments proving difficult to validate. Students are still required to attend physical testing centres in order to ensure strict examination conditions are applied. Whilst research has begun to propose solutions in this respect, they fundamentally fail to provide the integrity required. This thesis seeks to research and develop an e-invigilator that will provide continuous and transparent invigilation of the individual undertaking an electronic based exam or test. The analysis of the e-invigilation solutions has shown that the suggested approaches to minimise cheating behaviours during the online test have varied. They have suffered from a wide range of weaknesses and lacked an implementation achieving continuous and transparent authentication with appropriate security restrictions. To this end, the most transparent biometric approaches are identified to be incorporated in an appropriate solution whilst maintaining security beyond the point-of-entry.

Given the existing issues of intrusiveness and point-of-entry user authentication, a complete architecture has been developed based upon maintaining student convenience but providing effective identity verification throughout the test, rather than merely at the beginning. It also provides continuous system-level monitoring to prevent cheating, as well as a variety of management-level functionalities for creating and managing assessments including a prioritised and usable interface in order to enable the academics to quickly verify and check cases of possible cheating. The research includes a detailed discussion of the architecture requirements, components, and complete design to be the core of the system which captures, processes, and monitors students in a completely controlled e-test environment.

In order to highlight the ease of use and lightweight nature of the system, a prototype was developed. Employing student face recognition as the most transparent multimodal (2D and 3D modes) biometrics, and novel security features through eye tracking, head movements, speech recognition, and multiple faces detection in order to enable a robust and flexible e-

invigilation approach. Therefore, an experiment (Experiment 1) has been conducted utilising the developed prototype involving 51 participants. In this experiment, the focus has been mainly upon the usability of the system under normal use. The FRR of those 51 legitimate participants was 0 for every participant in the 2D mode; however, it was 0 for 45 of them and less than 0.096 for the rest 6 in the 3D mode. Consequently, for all the 51 participants of this experiment, on average, the FRR was 0 in 2D facial recognition mode, however, in 3D facial recognition mode, it was 0.048. Furthermore, in order to evaluate the robustness of the approach against targeted misuse 3 participants were tasked with a series of scenarios that map to typical misuse (Experiment 2). The FAR was 0.038 in the 2D mode and 0 in the 3D mode. The results of both experiments support the feasibility, security, and applicability of the suggested system.

Finally, a series of scenario-based evaluations, involving the three separate stakeholders namely: Experts, Academics (qualitative-based surveys) and Students (a quantitative-based and qualitative-based survey) have also been utilised to provide a comprehensive evaluation into the effectiveness of the proposed approach. The vast majority of the interview/feedback outcomes can be considered as positive, constructive and valuable. The respondents agree with the idea of continuous and transparent authentication in e-assessments as it is vital for ensuring solid and convenient security beyond the point-of-entry. The outcomes have also supported the feasibility and practicality of the approach, as well as the efficiency of the system management via well-designed and smart interfaces.

Contents

List of Figures

List of Tables

Acknowledgements

First and foremost, all praise and gratitude is due to Allah the All-Compassionate and All-Merciful for everything He has provided me throughout my life, in general, and for giving me the potential and patience to persevere and reach this stage of my PhD research, in particular. Without Him, I would not have achieved anything or even existed.

I also owe a debt of gratitude to my beloved parents (Nawal Saadallh and Dr Shakir Ketab) for their considerable encouragement and support, and passionate love and prayers for my success even though I have fallen short of being worthy of all what they do and have done for me. Any success that might be resulted, hopefully, should help me make them proud and happy of me. May Allah reward them the best.

My unreserved love, thanks and appreciation must go to my wife (Aysar Hasan) and children (Ali and Jana) who have been very patient, understanding, and inspiring to me throughout this endeavour, spending days, nights, and sometimes even holidays without me. Hope that the potential success of this research will compensate some of what they have missed. May Allah bless them.

A very special "thank you" goes to soul of my grandfather Ketab, my brave brother Rafal and all my family members for supporting me through my entire life.

This thesis would not have been completed on time without the invaluable guidance, wholehearted support, timely feedback and utmost professionalism from my Director of Studies Professor Nathan Clarke. I would like to express my special thanks and admiration to him. It has been really a pleasure and an incredibly rewarding experience to work with him and I am looking forward to continue doing so in future.

Very deep and special thanks also go to my supervisor, Associate Professor Dr Paul Dowland, for his insights and support. Moreover, I would like to thank all staff members in the Centre for Security, Communications and Network Research Group for their support.

I would like to thank all my friends and colleagues, either in the UK or in Iraq, who have contributed positively towards my progress by any means even if it was just a smile. Many of them deserve mentioning but it is difficult to state all the names. However, it is inevitable not

to express my sincere thanks to my brother-like friend Dr Abdulwahid Al Abdulwahid for all kinds of support he has provided throughout my PhD journey. I wish them all success in all their current and future endeavours.

Finally, I would like to acknowledge with thanks and appreciation the Higher Committee for Education Development in Iraq (HCED) and my employer, the University of Baghdad / College of Education for Pure Science – Ibn Al-Haitham / Computer Science Department.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee.

Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment.

This study was financed with the aid of sponsorship from The Higher Committee for Education Development in Iraq (HCED).

Relevant scientific seminars and conferences were attended at which work was often presented and several papers were published and prepared for publication in the course of this research project. Other research skills development courses were also attended.

Word count of main body of thesis: 69,305 words

Signed……

Date…….

1 Introduction & Overview

1.1 Introduction

Historically, since the late nineteenth century, correspondence and broadcast courses have formed the first distance learning shape before the emergence of the so called "digital age" (Bailie & Jortberg, 2009; Rovai, 2000). Over the last ten years, e-learning has played an important role in education (AL-Smadi et al., 2011) with a leading Virtual Learning Environment (VLE) provider reporting a user base of 70 million students and 1.2 million teachers across 7.5 million courses (IT Parks Update, 2014). Whilst e-learning has introduced flexibility and remote/distance-based learning (Prakash & Saini, 2012), there are still aspects of course delivery that rely upon traditional approaches (Mothukuri, 2012). The most significant of these is examinations (Wei et al., 2010).

"The issue of online cheating concerns many educators, particularly as more students take MOOCs for college credit, and not just for personal enrichment."

(New York Times, 2013)

Currently, in most higher education institutions, e-assessment plays vital role to enhance the learning process such as on-demand examinations, facilitating the marking process, or exam cost reduction. However, issues in e-learning security are still the biggest barrier to utilise e-assessment effectively (i.e. are the students taking the test actually the genuine/legitimate students doing it or are they cheating?). The lack of trusted approaches for authentication of students has been a vital obstacle facing e-learning developers (Levy and Ramim, 2007). Thus, e-learning environments should be provided with an adequate level of security and fault tolerance to ensure accurate performance. In order to overcome this, verifying the student's identity should provide the required security in e-assessments, and hence it currently occupies the highest priority in this regard. To achieve a secure online test, various authentication methods including passwords, smartcards and biometric authentication are used. Whilst research has begun to propose solutions in this respect, they fundamentally fail to provide the integrity required (Sabbah et al., 2012; Fadhel et al., 2011; Clarke et al., 2013). The suggested solutions to minimise the cheating behaviours during the online test have varied. However, none of the suggested systems, prototypes, or schemes described in the

literature thus far, can provide transparent and continuous authentication; and play the role of robust, secure, flexible, applicable alternative. Hence, there exists a gap in the current online examination regarding its security and it is a vital research area seeking solutions.

Therefore, this research will explore the feasibility of designing and experimentally validating a robust online monitoring environment that can provide the same or better levels of security than current physical invigilation provides. Furthermore, it seeks to research and develop a novel e-invigilator that will provide continuous and transparent invigilation of the individual undertaking an electronic based exam or test.

1.2 Aims and Objectives

The aim of this research is to explore, propose and evaluate a biometric profiling approach and a variety of security techniques which enhance the security for the e-assessments. In order to achieve this, this project is divided into the following objectives:

1- To review the current security provision within online assessments and better understand the risks associated with the e-assessment environment.

2- To critically evaluate a comprehensive review of biometric authentication approaches. Particularly the transparent biometric-based technologies and a gap-analysis on their feasibility to be used in the invigilation of e-assessment.

3- To design an architecture to support the aims of continuous, robust and transparent identity verification and range of security techniques on online assessments thereby ensuring security is maintained.

4- To implement and test a prototype of the proposed system to demonstrate its practical effectiveness.

5- Utilising the developed prototype with a number of participants to experimentally testing, evaluating, and validating the suggested architecture.

6- To perform a series of scenario-based evaluations, involving the three key stakeholders (i.e. experts, academics and students), to provide a comprehensive evaluation into the effectiveness of the proposed approach.

1.3 Thesis Structure

To fulfil the aims and objectives stated in the previous section, this thesis continues in Chapter 2 by presenting the current state of the art of e-invigilation strategies, starting with a general overview, and then exploring in more detail the current solutions for the problem of student monitoring during online examinations (covering commercial products and research into novel approaches).

Chapter 3 investigates the field of biometrics with a detailed historical review of the development and use of biometric techniques. The chapter discusses different aspects and principles regarding biometric acquisition and classification technologies. It divides the biometric characteristics into physiological and behavioural biometric approaches and provides narrative surrounding their application, strengths, and weaknesses. It builds upon the knowledge of biometric systems and presents an analysis of biometrics that have been used/proposed for invigilation of online assessments. Additionally, the study explores the use of transparent biometrics in solving some of the issues surrounding continuous identity verification.

Having established the key barriers to a successful e-invigilation system, Chapter 4 proposes an intelligent E-Invigilation of E-Assessments System (EIEA) architecture which incorporates the composite transparent authentication and security framework. The architecture has been designed around two core operational objectives: continuous multimodal biometric-based monitoring of the participant and system-level monitoring to prevent various forms of possible cheating. The chapter presents a detailed breakdown of the architecture, its core functionality and underlying processes.

To aid further investigation of the proposed architecture and enable a validation and evaluation, a prototype has been developed and is presented in Chapter 5. The chapter presents, in detail, the development and implementation of an EIEA prototype from the two perspectives of the key stakeholders (i.e. academic and student). It was developed not to be

complete operational prototype or to implement full commercial operational system but to provide sufficient functionality in order to address the research questions.

Chapter 6 experimentally explores the viability of the proposed EIEA system. A multiple scenario experiment involving 51 participants was undertaken to evaluate the usability and investigate the ability of the system to successfully identify cheating. The core research questions were identified in this chapter. It presents the methodology followed and results of the two main experiments (i.e. Experiment 1: Transparent & Continuous Biometric Identity Verification and Experiment 2: Targeted Attack). The operational considerations are also detailed.

Chapter 7 presents a series of scenario-based evaluations to provide a comprehensive stakeholder evaluation into the effectiveness of the proposed approach. To evaluate all dimensions of the EIEA system, the three separate stakeholders were identified: students, academics and experts.

Finally, Chapter 8 presents the main conclusions from the research, highlighting the achievements and limitations. Future research and development for this project are also suggested.

2 Literature Review of Invigilated E-Assessments

2.1 Introduction

E-learning has been supported by a massive number of providers utilising platforms to deploy various scientific, educational, or training and teaching course materials (Luminita, 2011). They provide a lower burden upon teachers, lowers room costs, reduces equipment and travel time for both students and instructors (Sumathi, 2010; Al-Smadi et al, 2011), thereby saving their time and increasing the student's scope of learning by giving them the opportunity to get an extensive spectrum of education facilities from content delivery to online examinations. However, e-assessment opens the window for candidates to do illegal behaviours during the assessment, this particularly in the absence of the instructor or non-bias monitoring. One reason for unsuccessful e-learning is the absence of fully trustable, secured, protected and cheating-free e-examinations (Hentea et al., 2003; Alwi and Fan, 2010; Flior and Kowalski, 2010; Apampa et al., 2010a; Marcus et al., 2008, Alotaibi, 2010). Many studies stated that cheating behaviours and illegal help are very common in education environment (Rowe, 2004; Dick et al., 2003). Reports suggest that more than 70% of the American students in the high school acknowledged they committed cheating in at least one exam (Bushweller, 1999). Yet, 95% of them have never been caught (Levy and Ramim, 2007; Rowe, 2004; Dick et al., 2003). Further studies highlighted about 75% of the students in colleges had cheated (Rowe, 2004; Dick et al., 2003). The situation is even worse in the e-learning environment (Sabbah et al., 2012), whereas about 74% of students admitted to cheating during the e-assessment, as it is easier than in traditional exams and might never be identified (Apampa et al., 2010a). While this problem can be diminished by employing physical proctors and asking the students to mandatory attend fully controlled classrooms, this tends to increase the burden and cost on both the teacher/inspector and student, as well as limit the growing scope of the remote education and training in general. Therefore, many researchers are currently focusing their efforts to specify and produce an effective e-invigilation system.

Authenticating test takers is a vital process in order to ensure their identity at test time (Hentea et al., 2003; Alwi and Fan, 2010; Flior and Kowalski, 2010; Apampa et al., 2010a; Marcus et al., 2008, Alotaibi, 2010). Generally, it can be achieved by utilising one or more of the following three fundamental approaches (Wood, 1977):

- Knowledge Factors: This method requires a user to know something unique (e.g. passwords, PINs, graphical passwords, and cognitive questions) that others do not know.
- Ownership Factors: In this method, a user should have some token that others do not have, for example, SIMs, smart cards, mobile phones, and hardware/software one-time password (OTP) tokens. Unauthorised user can only access users' information if they get the required tokens.
- Human Inherence Factors: Offer a very accurate means of authentication. They do, however, have weaknesses in that they can be intrusive, expensive and difficult to implement. They are also referred to as biometric authentication methods. They have been implemented into two main types (Flior and Kowalski, 2010): *Something the user is*, a highly reliable method for user authentication including but not limited to fingerprint, iris, retina or face. And *something a user does*, which is less reliable than the former method but generally could provide more user-friendly authentication such as: mouse dynamics, keystroke analysis or speaker recognition.

Current approaches require a user to intrusively provide an authentication sample (e.g. password or fingerprint) – to ensure someone does not impersonate the legitimate student. The poor use of passwords and PINs has been widely documented, with many laptop owners using simple passwords that dictionary attacks can crack in seconds (Denning, 1999). However, in circumstances where the user is complicit in the misuse, such approaches have a significant failing in that users know when and how to circumvent the system. Therefore, there is a need for authentication techniques that are not easily shared or given away (e.g. biometrics) and that go beyond initial login (i.e. the legitimate user can simply login biometrically and then leave), thus there is an essential need for continuous and multimodal biometric identity verification. Therefore, this research aims to establish an advanced authentication architecture capable of providing the increased security required for e-assessment and extending protection beyond point-of-entry as to ensure the identity of the user on a continual basis. Further to this continuous authentication (with the resulting system automatically identifying possible misuse), a second aim, that of providing transparent or nonintrusive authentication, is deemed imperative in order to minimise user inconvenience and increase subsequent user acceptance. By being able to authenticate a user without their knowledge, the integrity of the system can be automatically maintained and monitored

without the user's explicit interaction, until such time as the system deems an impostor is accessing the system.

2.2 Current State of Art

In prior literature, the number of suggested solutions to minimise the cheating behaviours during online tests have varied and have been categorised as: human proctoring systems, biometric-based solutions, system level security solutions, and commercial solutions.

2.2.1 Human Proctoring Systems

Physical proctoring in e-learning is the traditional method of (human involvement) invigilating (Figure 2.1), monitoring, or supervising examinees throughout online assessments. During the past ten years, many authors supported the idea of human involvement in monitoring online assessments (e.g. utilising/dedicating institutional examination centres). More recent arguments for this have been summarised by (Rovai, 2000a; Rowe, 2004; Marais et al., 2006). Some of the issues emerging from these findings focus specifically on the suitable low-technology approach for identification of any suspicious action that might occur during the online assessment in order to promote and maintain academic integrity. Moreover, many new studies, such as York (2014) and Farnese et al. (2011) found that these findings are consistent and in agreement with findings which showed that the possibility of candidate cheating in such circumstances is low in comparison with other means of online assessment invigilation.

Source: Missouri State University, 2016

Figure 2.1: Taking Proctored Exams on the MSU Springfield Campus

However, the above results differ from some published studies (Apampa et al., 2009). For instance, in a study which set out to determine physical presence of the student in e-assessment room/laboratory, where the inspector merely depends on the student ID card to verify the student physical attendance and giving permission to undertake the online test. And hence, if there is enough similarity between the photo of the presented student ID card and student's face, then the permission will simply be given to the student to participate in the e-assessment. In their review of this case, Apampa et al. (2009) highlighted a problem of similarity between candidates and the difficulty that an invigilator could face in order to differentiate between the lookalike students, family members, or the most significant confusing case which is the identical twins.

Additionally, in an investigation into invigilation literature, Apampa et al. (2010a) found that there is a possibility that an invigilator could conspire with the fraudulent student to allow cheating actions. Both the conspired impersonation and responding to human emotions are discussed in detail in many studies such as: (Moini & Madni, 2009; McCabe, 2005; Stuber-McEwen et al., 2009). These studies have demonstrated that this kind of academic dishonesty could open the door for further types of fraud activities, for instance, allowing another person to undertake the exam instead of the actual student.

There is no practical mechanism and full guarantee to prevent the examinee from looking at the screens of other examinees that sit next to him/her (Gilbert et al., 2009). However, there is a mitigation for this argument; in their studies, many researchers, teachers, and software developers have suggested various solutions including: question pooling, randomise a question order, shuffle the answer options within a question, adding time limits, employing mixed question styles, and/or asking for the seat numbers of the examinees (where each examinee will be given a random seat number to avoid the possibility of sitting in previously agreed places in order to carry out illicit cooperation). Therefore, if a test taker peeks at a monitor of another student neighbouring him/her or even the others' screens in the electronic exam room, it will look entirely different comparing with his/her own screen (Biella et al., 2009; Lu et al., 2013; Jung & Yeom, 2009).

In 2012, in Iraq, the ministry of higher education and scientific research has declared that both the computer-based English language test (e.g. TOEFL iBT) and computer abilities exam certificate (e.g. Internet Core Competency Certification (IC3)) are not required for Master or PhD degree acceptance, this because they could not rely anymore on such insecure

online exams which are mostly proctored by untrusted people with high cheating threats possibilities. In consequence, the ministry has developed and produced its own more secure and powerful online English language and computer skills assessments. They suggest relying upon traditional solutions such as using question banks, question pooling, and/or randomising questions orders (Baghdad University, 2014). Nevertheless, the proposed solution still requires direct human invigilation and student's attendance in a classroom in order to undertake the online test.

Prior to 2014, due to the high level of student cheating in both Test of English for International Communication (TOEIC) and Test of English as a Foreign Language (TOEFL) iBT tests that are equivalent to International English Language Testing System (IELTS), their adoption by the UK Border Agency (i.e. being one of the UK Border Agency accepted requirements to obtain the UK Visa by foreign people) has been ceased as they are untrusted computer based exams.

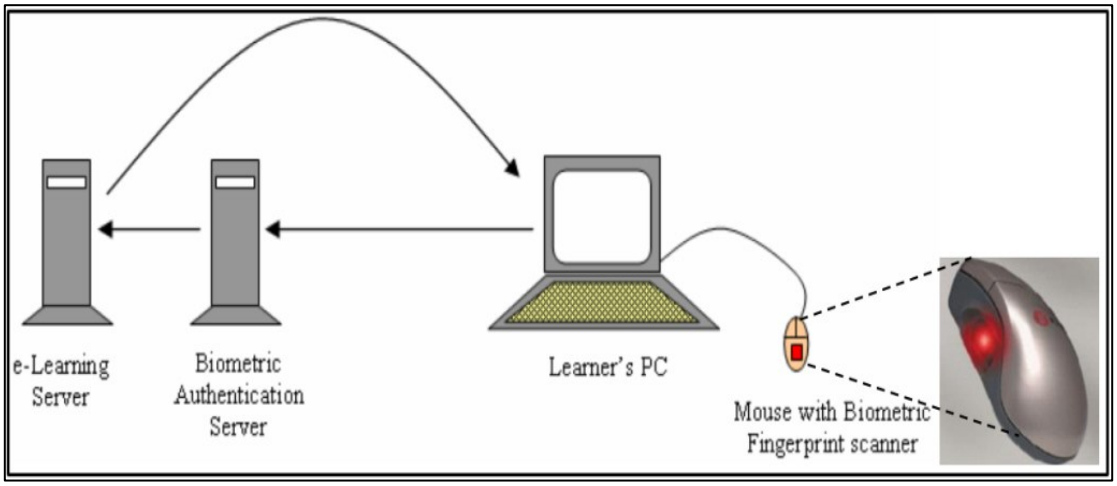
> *"ETS is no longer licensed by the Home Office to award test of English for International Communication (TOEIC) and Test of English as a Foreign Language (TOEFL) iBT tests for UK immigration and nationality purposes. U.K."*
>
> (UK Border Agency, 2014)

2.2.2 Biometric-Based Solutions

In order to provide a better level of security, many researchers tend to involve biometrics utilising the flexibility and variety of currently available recognition techniques in this area. Generally, most researchers have relied upon one or more biometric technique of the candidate during the exam such as voice recognition, fingerprint recognition, keystroke analysis, or mouse dynamic recognition. However, the essential question here is whether these biometric approaches are extending protection beyond point-of-entry as to ensure the identity of the user on a continual and transparent basis or not. According to the biometric modalities employed in the proposed systems, the research in this context is also branched into intrusive and non-intrusive approaches.

A considerable amount of literature has been published on biometric schemes in online examinations. They depend on one information source to decide whether to give permission to the candidate to participate in the assessment. A number of studies have investigated

utilising physiological biometrics only aiming to verify the legitimate student robustly (e.g. at the beginning) without achieving principle of transparent authentication such as: fingerprint recognition, iris recognition, head geometry (Hernández et al., 2008; Apampa et al, 2010c; Onyesolu et al., 2013; Levy & Ramim, 2009; Bal & Acharya, 2011). Some of these physiological biometrics (e.g. fingerprint – see Figure 2.2), to a large extent, can be considered as intrusive techniques (none user-friendly), this due to the need for explicit authentication in order to implement the authentication process, in addition a direct connection with the biometrics reader is required. For example, to collect the data for fingerprint recognition, the user needs to touch his/her fingertip to the sensor, whereas the face recognition technique, for instance, can be achieved passively/implicitly (even without the user knowledge). Further studies were separately presented relying only on non-intrusive behavioural biometrics such as keystroke dynamics (Flior & Kowalski, 2010). The commentary that follows describes the key achievements and milestones that have taken place in this regard.



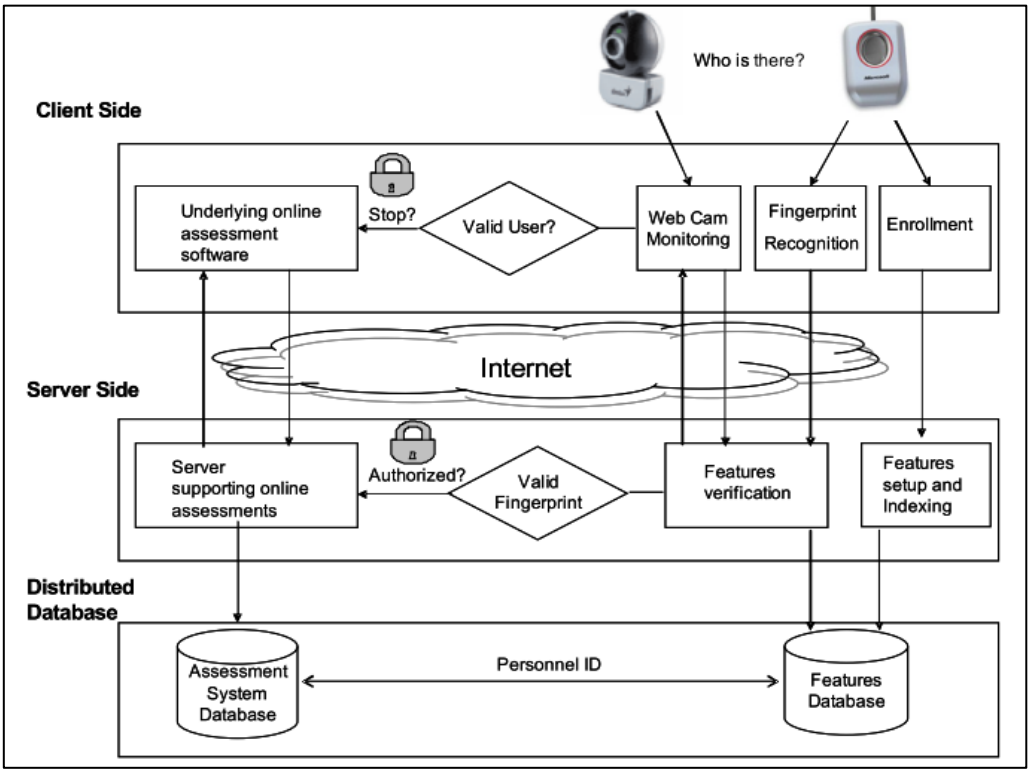
Source: Sabbah, 2012

Figure 2.2: Example of Single Biometric System, Fingerprint Recognition on Real Time in Online Assessments

A number of studies have found that fingerprint biometric technology is a suitable well-known solution for candidate authentication during e-assessment (Hernández et al., 2008; Levy & Ramim, 2009). Sabbah, (2012), for example, argues that these intrusive biometric modalities are suitable for examinee login stage and to solve the problem of "who is there?" in order to verify the identity at the beginning of the test. Although it can be utilised in solving the problem of "is the student really who they say they are?" (e.g. the user is randomly asked to authenticate), but, this is not a practical alternative as it distracts the

attention of the student during the online test. However, instead of employing an intrusive fingerprint method, other studies argued that face recognition biometric technology as relatively new and more user-friendly could provide a better alternative (Zhao & Ye, 2010; Apampa et al., 2010c; Mothukuri, 2012).

Hernández et al. (2008), proposed a prototype uses a fingerprint biometric authentication approach to deal with or overcome the problem of student identification at the beginning of the exam together with synchronised student continuous observing using web camera until the end of the online test (as shown in Figure 2.3). They involved a random sample of 102 high school students for fingerprint enrolment, the experiment accomplished a robust performance with False Acceptance Rate (FAR) of 0.01% and False Rejection Rate (FRR) of 2.91%. Furthermore, in order to improve the performance of the system, some ordinary mechanisms have also been recommended, namely: randomise questions orders, shuffle the answer options within a question, and adding time limits. However, this study did not explain the continuous video monitoring during the exam time properly. Moreover, the use of fingerprint does not support the principle of continuous and transparent user authentication beyond point-of-entry.



Source: Hernández et al., 2008

Figure 2.3: Structure of Fingerprint and Video-Monitoring in E-Assessments

Onyesolu et al. (2013) suggested an approach to enhance secure electronic assessments, through a combination of fingerprint biometric system for identification during the online examination (as illustrated in Figure 2.4) and distributed firewall techniques to monitor candidates and control network packets of all machines incorporating the traditional username and password for verification. Once the student accomplished fingerprint enrolment, he/she will be identified with biometric system by verifying their fingerprints with those captured earlier during the enrolment stage. Then, they will log in with their Username and Password (for authentication) which were assigned to them after a successful biometric identification. An agent will then start extracting the fingerprint using a fingerprint scanner at every second to ensure that no other person could take the assessment on another student's behalf. However, the authors have not tested their proposal empirically. Furthermore, the idea of keeping student's finger continuously on the fingerprint scanner for verification suggests an intrusive mechanism.

Source: (Onyesolu et al., 2013)

Figure 2.4: Fingerprint Enable USB Device

A cost effective iris recognition authentication approach has been suggested by Bal & Acharya, (2011) as an endeavour to overcome the problem of impersonating the test taker. They tried to employ a unimodal biometric solution (iris recognition), thereby proposing to extract the image of the iris from the enrolment photograph of a candidate facial image. This suggested technique would help the inspector to authenticate the candidates besides tracking them during the online assessment. Whilst the image acquisition occurs in the users' computer in order to capture the image of the eye, for further processing, the image will be sent to the server along with the student ID. To test the uniqueness of the suggested iris

recognition method, 10 random individuals are selected. Images of both eyes of each individual are taken, the experimental result shows 100% uniqueness of iris. Nevertheless, this suggested system could face many difficulties such as the traditional human academic dishonesty via providing the student unauthorised help, and cheating from the closest students or even a misuse of forbidden Internet and computer resources during the real time of e-assessment. Furthermore, the areas that are wrongly identified as iris regions in the segmentation stage (in the iris features extraction process) will corrupt biometric templates resulting in very poor recognition performance, as this is a crucial step in the biometric system component which comes after the capturing step. In addition to previous limitations, there is a technical problem of this scheme that the test taker's eyelid might shade about half of the iris which acts as a big barrier that prevents accurate required image acquisition (Bal & Acharya, 2011; Apampa et al., 2009; Besbes et al., 2008; NSTC, 2006h; Tayal et al., 2009; Tayal et al., 2009a; Babich, 2012). This is attributed to the fact the student mostly looks at a specific position of the monitor during reading, writing or searching for a correct answer among multi choices. Thus, the interacting examinee should look at the camera directly which typically is located at the top of the screen, which adds a burden on the test taker and distracts their concentration on the exam question. Therefore, although they tried to make it non-intrusive, they need for a user to look at the camera periodically (intrusively) in order to achieve the authentication.

Irfan et al., (2009) presented a face recognition based monitoring tool for online e-learning systems. They proposed image normalisation and feature extraction using the Discrete Cosine Transformation (DCT), the Karhunen-Loeve Transform (KLT), and Radial Basis Function Network (RBFN) on the JPEG image. The method was tested on the ORL database involving 400 images of 40 subjects, 200 images were used as samples and another 200 images were used for testing. 5 images were randomly chosen as training samples and 5 images were chosen as the testing samples. The experiment accomplished an error rate of 2.45% with fast recognition time (0.055 sec.). However, the study lacked a real participant face recognition, as they utilised JPEG image from a dataset. Furthermore, the authors ignored the principle of continuous authentication in their proposal.

Two proposed approaches in the literature offer applicable suggestions to achieve user authentication within an online test, both employed behavioural biometrics (voice recognition and keystroke dynamics). The first was a low-cost and effective voice recognition mechanism

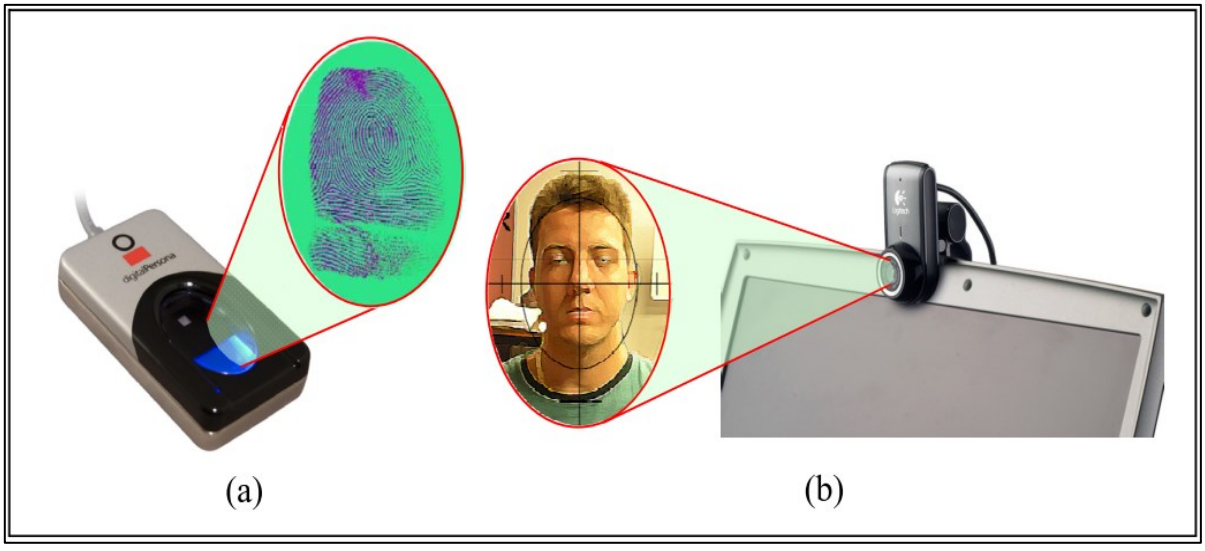
proposed by Hayes & Ringwood, (2008) and supposed to be sufficiently accurate to act as an effective deterrent against plagiarism associated with the submission of assignments for e-learning programs. A prototype of student authentication system has been designed for use with a graduate e-learning program to authenticate a telephone-based oral examination. A sufficient (97.5%) final classification accuracy has been achieved using amendable classifier. The second is a method for providing continuous biometrics user authentication in online examinations via keystroke dynamics, rather than using a classic user-ID/password authentication approach, in order to prevent any other individual taking the exam for the legitimate student (Flior and Kowalski, 2010). They have developed software system which combines HTML, PHP, MySQL, and JavaScript to create an implementation for managing an e-assessment where keystroke dynamics are employed for student authentication. The implementation of keystroke dynamics continuous authentication needs to be accomplished using PHP and JavaScript embedded in HTML.

In another study which was set out to determine examinee authentication scheme utilising one of behavioural biometrics, Kikuchi et al., (2008) found that using biometric handwriting-based samples by applying the localised arc pattern method is a good alternative which confirms the examinee identification periodically during the test when using pen tablets. As a result of their experimentation, they argued that around 80% of the test data accurately identified the writer. Although most kinds of behavioural biometrics provide lightweight and transparent authentication methods, there is a dire need to improve the robustness of large-scale systems (Levy & Ramim, 2009), and to overcome the problem of instability of human behaviour such as changing mood, health, and environment which leads to continuous changing in stored templates (Araújo et al., 2005; Niinuma et al., 2010; Teh et al., 2010; USMA, 2012; Apampa et al., 2011; Tayal et al., 2009a; Clarke, 2011). Some people might behave differently under pressure, the health could impact the human behaviour if it changed negatively, and the environment might also play a role such as a student could perform differently if he/she takes the test in a classroom versus at home.

In an investigation into biometric identification and authentication, (Jain et al., 2000; O'Gorman, 2003; Weaver, 2006) found that biometric approaches, to some extent, suffer from the likelihood of being spoofed or faked (e.g. silicon fingerprint). Furthermore, due to these limitations, analysts and studies including (Das, 2011; Mir et al., 2011; Ross & Jain, 2003; Tsalakanidou et al., 2007; Jain et al., 1997) argue that the strategy of a single

biometric modality has not been successful for candidate authentication in online assessments. Hence, alternative studies have suggested utilising more than one modality in order to enhance the performance, as relying on more than one biometric trait could acquire more secure and reliable online assessment (Rabuzin et al., 2006; Sabbah et al., 2012; Software Secure, 2013; Asha & Chellappan, 2008; Clarke & Furnell 2007; Levy & Ramim 2009; Sabbah et al., 2012; Ross & Jain, 2003).

Even though it is a developing and interesting technology, multi-biometrics has not been suggested widely in many studies regarding e-learning, therefore, there is limited literature that could be drawn. In general, if special devices are needed on the end-user side; then the biometric solutions could add significant cost to the system (Ullah et al., 2012). In 2009 a theoretical model has been proposed by Levy and Ramim to investigate into the multi-biometric scheme to authenticate students during e-learning activities, including (a) a fingerprint scanner and (b) a Webcam which fits on the top of computers for head geometry scanner (Figure 2.5). Nonetheless, in this approach, further to the intrusiveness of the proposed fingerprint biometric, rather than focusing on practicality, security, applicability and performance of the suggested strategy, the study was merely interested in students' acceptance of multimodal biometric systems for verification throughout online assessments.

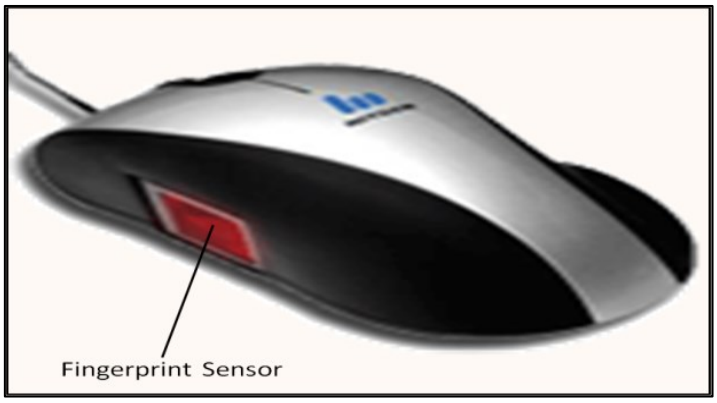


Source: Levy & Ramim, 2009

Figure 2.5: Bimodal Method to Authenticate Students during E-learning Activities

In an extensive study, Asha & Chellappan (2008) recommended merging behavioural and physiological biometrics by using mouse dynamics along with fingerprint recognition (both together in a single mouse device with fingerprint scanner), utilising the fact that the majority

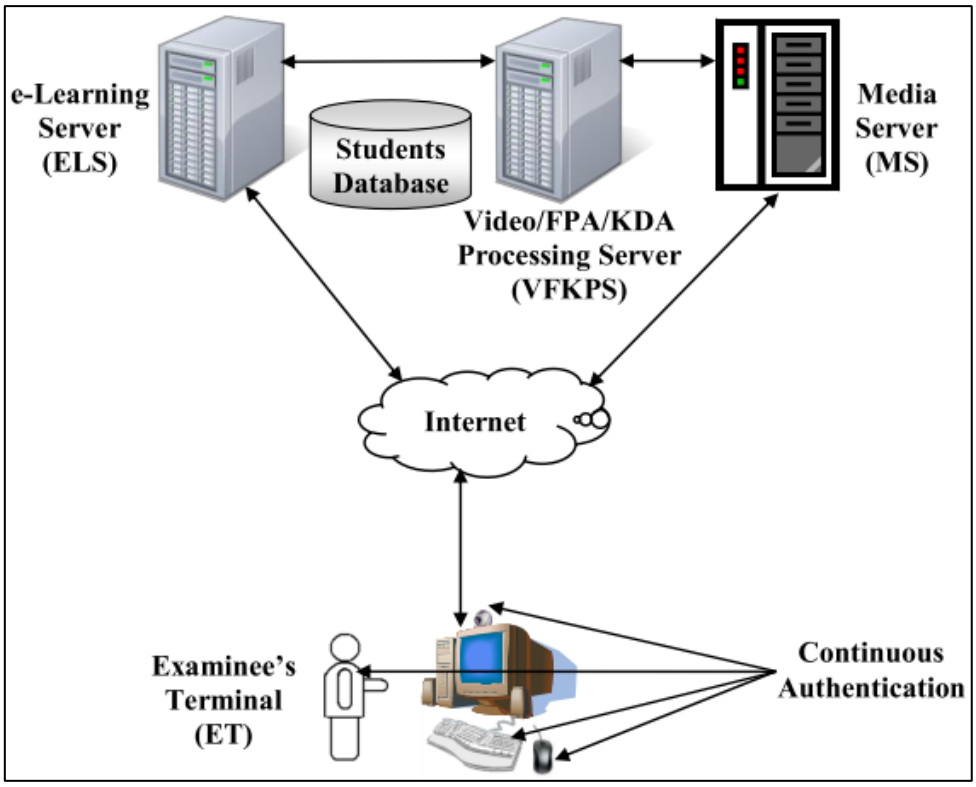
of user interactions with computers are being accomplished using the mouse interface. Therefore, in this study, they proposed using the mouse fingerprint detector to provide continuous checking of user identity, and for higher anti-spoofing scheme, they suggested employing the mouse dynamics itself to minimise any potential illegal help by somebody sitting next to the user (Figure 2.6 illustrates this dual biometric authentication device). Yet, the last assumption, particularly, was not a satisfactory suggestion. Many practical studies argue that the required time for data collection of mouse dynamics is very long to complete which opens the door for suspicious student activities during these critical lost intervals (Ahmed & Traore, 2007; Bours & Fullu, 2009; Stanić & Croatia, 2013; Shen et al., 2012; Jorgensen & Yu, 2011). The method also restricts the student to continuously touch the mouse reader in order to accomplish the continuous fingerprint authentication, in which produces intrusive action. In addition, the system does not take into account other problems including securing the environment around the student (e.g. sounds).



Source: Indeamart, 2014 (Modified)

Figure 2.6: Dual Biometric Authentication Device

An approach called SABBAH (Figure 2.7), which employs continuous bimodal biometric authentications mechanism depending on physiological biometric which is fingerprint features for log in and for continuous verification, and behavioural biometric which is type rhythm technique to ensure that the real examinee is the one who is typing in essay questions combined with automatic video matching scheme (for student in the log in), has been proposed by Sabbah (2012) as an upgrade prototype for a previously suggested approach by the same researcher.



Source: Sabbah, 2012

Figure 2.7: Structure of SABBAH e-examination model

This approach suffers from many limitations, despite the fact that suggesting fingerprint modality adds intrusiveness to the system, it also needs additional hardware in order to achieve the principle of continuous authentication (i.e. fingerprint scanner); furthermore, many additional requirements are also needed including: very high-speed and stable Internet connection (particularly at peak times), servers with higher processor speed, and larger memory and storage/disk space. Furthermore, the implementation of automatic video matching is very difficult and its algorithms need more development, and finally, the study does not provide any empirical evidence of the performance for both the fingerprint and the keystroke dynamics authentication.

An analysis of the above research on the biometric authentication has been undertaken and summarised in the following Table 2.1.

	Author(s)	Multi/Single Modality	Biometric Modalities	Performance (%)	Participants	Type	Continuous Authentication	Transparent Authentication
1	Hernández et al., (2008)	Single + Video Monitoring	Fingerprint	FAR 0.01 FRR 2.91	102	Simulation (Random Individuals)	No	No
2	Onyesolu et al. (2013)	Single + Firewall Security	Fingerprint	-	-	Conceptual	Yes	No
3	Bal & Acharya (2011)	Single	Iris	Accuracy 100	10	Simulation (Random Individuals)	Yes	No
4	Irfan et al., (2009)	Single	Face	Error Rate 2.45%	40	Images from DB	No	-
5	Hayes & Ringwood (2008)	Single	Voice	Accuracy 97.5%	4	Simulation	No	No
6	Flior & Kowalski (2010)	Single	Keystroke	-	-	Conceptual	Yes	Yes
7	Kikuchi et al., (2008)	Single	Handwriting	Accuracy 80%	4	Simulation	Yes	No
8	Levy and Ramim, (2009)	Bimodal	Fingerprint Head Geometry	-	-	Theoretical	Yes	No
9	Asha & Chellappan (2008)	Bimodal	Fingerprint Mouse	-	-	Conceptual	Yes	No
10	Sabbah (2012)	Bimodal + Video Matching	Fingerprint Keystroke	-	94	Survey (Conceptual)	Yes	No

Table 2.1: Biometric-Based Solutions

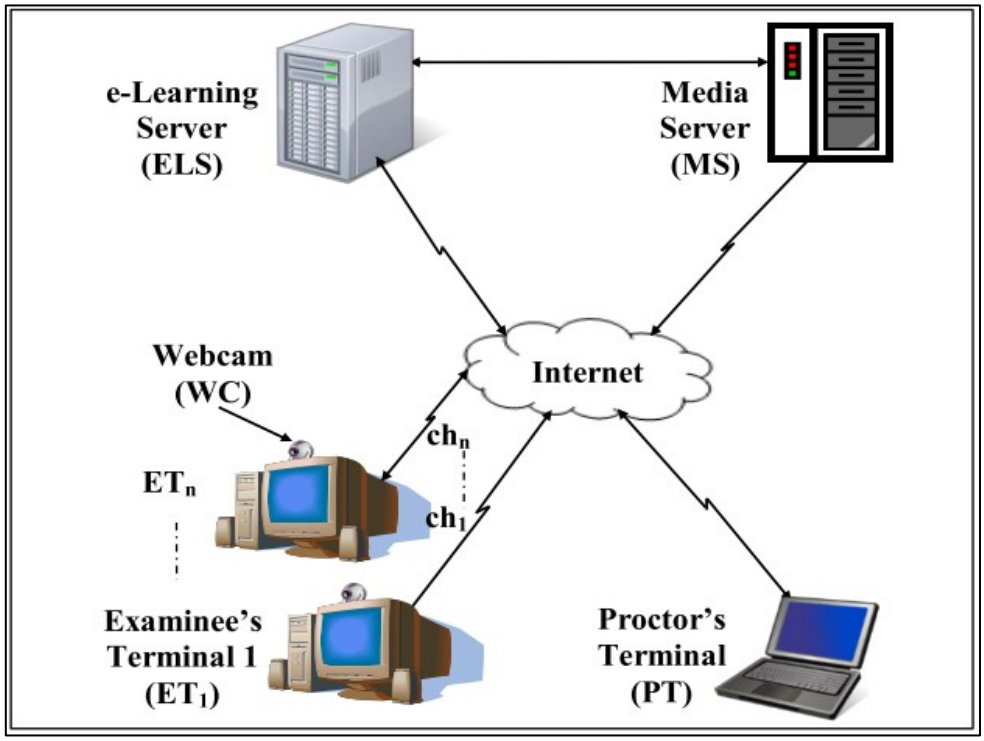
From this table, neither the proposed single-modals nor bi-modals biometric approaches so far could implement/provide both continuous and transparent authentication.

2.2.3 System Level Security

There are a variety of different controls that have been taken depending upon the nature of the platform or who has the control on the platform. Studies explored non-biometric-based countermeasure solutions that also introduced to help minimise cheating or provide restrictions of the illegal/unauthorised assistance during the e-assessment. For instance, using only video or direct monitoring as the simplest method.

Generally, the approach of live/direct or real-time monitoring of student activities can support the security side of various types of online assessments (Hernández et al., 2008; Ko & Cheng,

2004). It has been shown that one of the most effective of this is video monitoring of examinees during the electronic examinations (Lin et al., 2004). Sabbah (2012) endeavoured to suggest two alternatives solutions models for a secure electronic test system, one of them is a proctor-based model named Interactive and Secure e-Examination Unit (ISEEU – see Figure 2.8), this system relies on video recording using a camera settled in front of each student in the class.



Source: Sabbah, 2012

Figure 2.8: Structure of ISEEU Model Using a Webcam

The model proposes that an examinee is connected to a media server (MS) through the Internet via a webcam attached to his terminal (ET). The MS, in turn, creates a channel (chn) for each group of examinees to broadcast exam sessions to their proctor through an e-learning server (ELS). Each examinee's session is streamed through his/her channel, and all the video streams appear on the proctor's terminal (PT). For evaluation, a quantitative online survey has been conducted, where a questionnaire has been designed and distributed to a target sample including academics, students, and experts. However, the study concluded that video monitoring alone cannot stop cheating when detected since it lacks interaction. Also, it fails if the webcam is removed or turned to another object. Furthermore, the approach failed in scalability (33.3%) feature, where only security is scalable since it is managed by a proctor. Performance and storage failed due to more demand on them when the number of concurrent

examinees increases. Its feasibility also failed (43.8%), since economic feasibility is much affected with paid proctors as in the traditional scheme, and legal/cultural feasibility failed for the same reasons of usability. Moreover, the system requires manual intrusion, and hence, it is not fully automated; and if the web camera stops working, or intentionally removed by the examinee, the exam will be paused.

Ko & Cheng (2004), proposed capturing short video clips versus full video streams in order to reduce the bandwidth as the video data stream has to share the same channel of the e-assessment system merely to prevent cheating. They utilised a camera at the student computer to capture the student face and posture at random intervals (for two second) during the test – as they will not know when the videos will be captured (the transmission of these short videos at random times would aid to save network bandwidth and reduce the workload of the server), the captured videos will then be sent back to be saved on the system server in order to be reviewed by the teacher. However, the adoption of traditional username and password strategy as part of the system security could open the window for impersonation of examinee's personality by others. Furthermore, they involve impractical monitoring proposal, as the system still needs the teachers/inspector to review all these recorded videos just to ensure there is no unfamiliar or suspicious behaviour which might have been occurred by the examinees, this could add burdens on the teacher or online examiner, especially when there are hundreds or even thousands of students within or outside the education systems.

A number of other researchers have explored a variety of other areas with regards to online assessment. In 2004, Pan et al. proposed a system which utilised the distributed firewall techniques and centralised security policy management as a barrier in front of any network attacks and cheating to reach a secure e-assessment. Moreover, Carlisle & Baird, in 2007, proposed the RAPTOR assessment environment as a convenient and cost-effective approach which enables each test taker to insert a bootable CD in order to run the online exam using his/her own portable machine. Furthermore, in the next year, another paper into online examinations security, Ko & Cheng (2008) claimed that the use of Iomega Zip bootable disk which contains all the necessary files for conducting the exam is more flexible, easier, and more secure. In 2012 Ullah et al. (2012) published a paper in which they described a scheme to secure the e-assessments using a method called profile based authentication framework (PBAF) depending on the enrolment activities and challenging questions to build such profile, in addition to a user-id and password. They argued that this method is more feasible

than the widely suggested biometric authentication approaches by other writers. During the authentication process, once providing user-id and password by the student, the system presents random challenge questions. When the challenge questions are answered, the framework invokes the authentication process to verify the student's identity against profile answers. However, this approach has some well-known issues with regards to usability but moreover does not prevent a student who is complicit in the cheating.

Even though all these proposed systems are suitable for securing electronic examination environments, they are still limited for only narrow scope of online exams which basically are designed for.

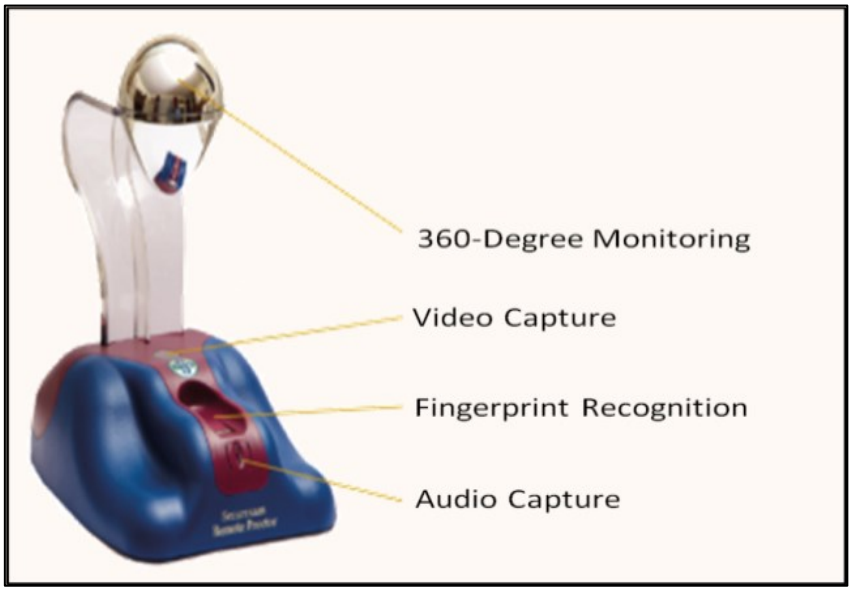
2.2.4 Commercial Solutions

Commercially, there are a number of companies that currently produce solutions for the monitoring of online assessment:

Software Secure: This company has developed many products, including Remote Proctor PRO, Securexam Browser, Securexam Student, and Remote Proctor Now (Software Secure, 2017). This company argues that students can take tests at their convenience anytime and anywhere using their computer and a webcam (Software Secure, 2011). Currently, they intend to expand their services to cover all types of examination including the variety of assessments in the educational institutions, for instance, high schools, colleges, or universities (Software Secure, 2008) and to ensure secure and convenience online assessments of certification organisations. Although, the system provides a level of authenticity, it still requires a level of human proctoring in order to tackle any potential cheating, this, in turn, breaks the principle of automation (Clarke et al., 2013). Additionally, they emphasise that: “the real-time nature of the capture is storage and bandwidth heavy”.

Moreover, the Securexam Remote Proctor System, illustrated in Figure 2.9, represents a leading attempt to simulate a live invigilator, giving a chance to the examinee to take the online exam wherever and whenever he/she wishes, and ensuring the academic integrity during the e-test, created by Software Secure company. The device contains a fingerprint authentication to verify the identity of the test taker, a camera installed under conic mirror to grasp 360-degree view monitoring of the room in which the exam conducted, and a microphone to record all sounds. While this system acts in a manner alike real and continuous proctoring, the suggested fingerprint recognition model could be feasible to be used within

the classroom, but it would be very expensive to suggest each student to buy a hardware device in order for merely takes apart in online exam. Furthermore, in an analysis of current available solutions for online assessment, Rosen & Carr, 2013, report: "The image is, however highly distorted and does not cover the ceiling of the test room", therefore, as shown in Figure 2.10, they developed a robot to achieve the same goal but they claimed it is cheaper and provides better performance than Securexam Remote Proctor System which has been suggested by Software Secure company. However, it is also impracticable proposal, due to additional attached devices, which required to be built and dedicated for each participant, furthermore, this would add further cost and unclear practicality/standardisation of the final product. Having said this, it is evident that neither these last two systems are feasible to be used in various online examinations environment.



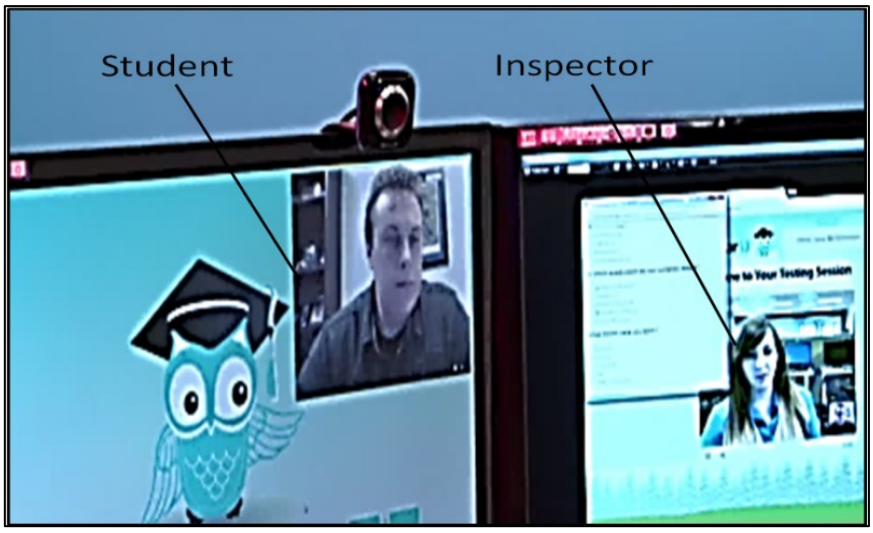
Source: Software Secure, 2011 (Modified)

Figure 2.9: Securexam Remote Proctor System

Source: Rosen and Carr, 2013

Figure 2.10: Prototype of the Exam Proctor Robot

Respondus: The company offers a product that promotes a secure, convenient, and integrated bases for online examinations using a Virtual Learning Environment (VLE) (Respondus, 2014), Figure 2.11 illustrates how the Respondus company monitors the candidates, as the student needs to take online test at predefined time in any location (e.g. using a computer with webcam at home) while an employee in the company verifies the student's identity in the beginning and then continuously monitors him/her. In order to reach the targeted level of security, a list of features have been adopted by the Respondus similar to Software Secure company to control the entire system and prevent or observe the suspicious activities during an e-assessment, including: preventing test takers from accessing unauthorised applications or websites prior and during the e-test, minimising screen, print, print screen, any capturing functions, copy, cut, paste, messaging, screen-sharing, running network monitoring applications, right-click, function keys, browser menu, and many other restrictions.



Source: Respondus, 2014 (Modified)

Figure 2.11: User Monitoring in Respondus Company

Coursera: it is an education platform that offers online and secure learning that has been provided to 108 universities partners and 622 courses around the world for free (Coursera, 2014). Furthermore, the company rely on the behavioural biometrics of test taker utilising keystroke authentication measures such as key hold down interval, typing speed and error patterns to verify the student's identity.

Kryterion: Another famous security company and a leader in live e-assessment proctoring, test development and delivery, item banking, and distance based video observation of examinees science 2001 (Kryterion, 2014a). In addition to continuous video and audio observing, the testing platform of the company provides keystroke biometrics as an approach to append further examinees' identity verification depending on a unique typing rhythms behaviour, facial recognition to match the taken photo during enrolment stage with the photo captured at the exam launching, and System Lockdown which permits only authorised and system level procedures to run (Kryterion, 2014b). For online students proctoring, Kryterion produces Webassessor (Kryterion, 2014c).

However, from criticising point of view, all the above "commercial" online assessment solutions would appear to be over ambitious in their claims. Hence, these companies to some extent fail to accomplish the required level of security and integrity. There is no product fully applicable on all currently used operating systems; most of these systems are limited to specific versions of Windows and Mac operating systems. Currently, with the continuously growing number of the virtual machine that could operate deferent kinds of operating

systems, perhaps the most serious challenge of these products is the probability of running them using these widely deployed applications. In addition, it is not always a good idea to lock out most software packages (which is the policy that followed by these companies in order to enhance the security principle) such as image processing programs, computer programing, statistical analysis, text editors, or any application that could give the teacher an opportunity to write different types of questions according to the curriculum or subject needs other than traditional questions styles offered by Learning Management System (LMS) (Percival et al., 2008). Moreover, neither Coursera nor Kryterion current products are offering continuous observing of the online exam actions (Rosen and Carr, 2013).

Fundamentally, in such authentication approaches that have been provided by a third-party service vendor, the sensitive students' information and biometric data (e.g. fingerprint, face, and voice recognition) are managed and stored on a third-party vendor's servers. The results of a survey conducted by Levy et. al., (2010), showed a clear indication by e-learners participants that they are significantly more willing to provide their biometric data and intending to use multibiometrics when provided by their university compared with same services provided by a third-party vendor such as Remote Proctor™ by SecurExam. 56% of the subjects indicated that they agree or strongly agree to use fingerprint biometrics during an e-test if it is managed by their university compared to only 19% if it is run by a third-party vendor. Furthermore, 52% of the participants specified that they agree or strongly agree to deliver their audio and video (via Webcam) during an e-assessment to their university compared to only 21% to a vendor.

2.3 Discussion

The literature has identified several challenges toward the current solutions for e-assessment in both remote and proctored room environment. One barrier is that some cultures or people live in specific countries oppose the idea of live or online video monitoring or even capturing their photos including the biometric features (Sabbah, 2012; Mahmud and Gope, 2009). In the distance-based examinations, the test taker may exist in drastically different environments, such as: a room in his/her own home, an office in the working place or even in a dedicated classroom for online examinations, resulting in challenges over determining or controlling the student actions, because there are more cheating scenarios that exist where the environment makes it easier to cheat.

The very poor Internet services or bandwidth, in many developing countries, have become a traditional barrier for online or real-time video recording or monitoring during the assessment (Mahmud and Gope, 2009). Some systems require room checking only in the beginning of the test through the webcam in order to ensure the security; however, there is no guarantee that this room will be secure anymore for the rest time of the exam, as easily the unauthorised help might be provided at any time. Furthermore, with room checking process, some students might feel uncomfortable due to the lack of privacy.

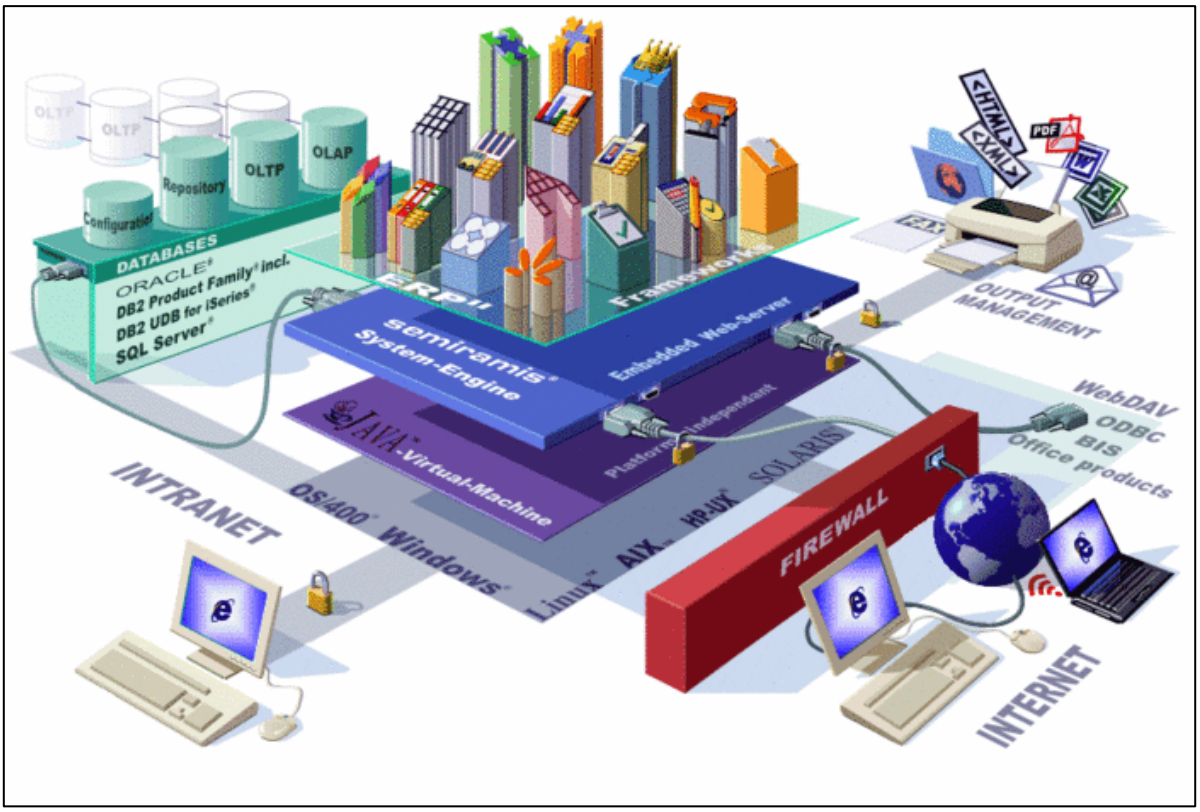
With the growing number of free Virtual Machine programs, the ability to run the online test through them represents a big challenge (Willems and Meinel, 2012). For example, the candidate, during the exam time, could run another operating system on the same computer being used for taking the test. Therefore, there is always a need to ensure fixing this problem.

Most proposed solutions involved additional costs, as in many cases there is a hardware or software requirement that would introduce a cost on the student in the case of remote-based assessment (Pleva et al., 2016). Moreover, the installation of additional equipment could bring further burden on students. Incompatibility between different devices should be avoided (Biella et al., 2009). Furthermore, in the case of classroom or testing centre, the equipment needs to be installed for every student going to take the e-test. In some institutions, there is a high risk of failure or theft possibility of equipment if it has been installed in a lab (Biella et al., 2009). In addition to, the required cost for covering the additional wage of a person who has been employed for the administrating/reviewing/proctoring the real-time or the recorded videos. In some colleges, for compressing the costs/expenses, they would trust inexperienced proctors thereby, for example, live/video proctoring sessions. They might also rely on waged students to invigilate other students taking online assessments. Indeed, there are no formal requirements for the person who takes part in most live proctoring. Therefore, giving an unknown or inexperienced proctor such high authorisations of control and supervision seems very risky for both institution and test taker (Gao, 2012). Furthermore, analysis of the feasibility and applicability of video monitoring showed that employing remote invigilator will be quite expensive (Rosen & Carr, 2013).

One of the functionalities of an e-assessment system is to offer secure exams that are void of intrusions. Having said this, it is evident that an exam taker should not be interrupted for the duration of the test except in explicit situations. Clarke and Furnell, (2007), for example, suggested transparent or non-intrusive continuous authentication employing behavioural

biometric techniques. This method has the effect of moving away from a Boolean authentication result to a more meaningful and appropriate confidence measure. However, the current solutions tried to give the robustness (security of the system) more weight over the non-intrusiveness, by involving fingerprint recognition technique, for instance. Others preferred ensuring user convenience avoiding the intrusive techniques (e.g. utilising keystroke recognition). Nevertheless, none of them was able to balance both essential requirements thus far. Therefore, further to the specified limitations across this chapter, the proposed methods have not succeeded to accomplish a realistic, secure, and convenient continuous and transparent authentication in the e-assessment environment.

To further evidence the need for this research, whilst undertaking it, the author was made aware of a new European funded project looking to achieve many of the same goals as this research (The Open University, 2016). An Adaptive Trust-based e-assessment System for Learning (TeSLA) (see Figure 2.12) was started in 2016 (The duration of the project is 3 years, starting on January 2016 and ending on December 2018 – notably after the completion of the bulk of this PhD). The project is financed by the European Commission under the Horizon 2020 Research and Innovation Framework Programme, with a total budget of 7,283,092.50 EUR. Relying on the combination of new technologies in the field of authentication (e.g. 2D facial recognition, speech recognition, keyboard analysis) and authorship, they are trying to develop a system that facilitates e-assessment in such a way that it is guaranteed that the legitimate student has logged in (authentication) and personally takes the exam (authorship). In the development stage, they are also considering quality assurance agencies in education, privacy and ethical issues and educational and technological requirements throughout Europe.



Source: The Open University, 2016

Figure 2.12: TeSLA Technical Architecture

2.4 Conclusion

Due to the current security problems in e-assessment and the growing number of institutions interested in offering online education, studies across the world have tried to bridge this gap involving a variety of approaches. However, student authentication and identity verification remains an outstanding issue. Whilst the majority of the research has focused upon point-of-entry authentication, they fail to appropriately accommodate for motivated students who wish to cheat. For studies focused upon security, real-time monitoring of students is typically proposed; however, whilst potentially effective, this results in hours worth of video and other content for an academic to review to ensure cheating has not taken place. With large numbers of students, this quickly becomes a very inefficient and un-economical approach. The use of transparent authentication employing biometrics would improve both the requirement for a robust authentication mechanism and the student's need to eliminate any inconvenience during the authentication process. Moreover, it would provide the academic with a prioritised set of results of who to investigate, providing in a more timely and economical solution.

3 Biometric Authentication

3.1 Introduction

This chapter focuses on presenting and discussing the human biometric modalities authentication, as it would be prudent to investigate this further with a view to understanding how they work, what error rates are and how robust they are against targeted attack. The chapter commences by providing the generic biometric definitions, then an overview of the history and standards of biometrics are outlined. As well as discussing its essential technical details including requirements, operational modes, components and performance. An analysis of two sets of biometric techniques is presented, the first are those that have been proposed to be used in the e-invigilation systems, and the second are the modalities that could have some role in the future in this area. A review of continuous and transparent authentication including some key relevant frameworks is also presented. Finally, the chapter ends with a summary of biometric transparency, applicability, and user satisfaction in online assessments.

Through the ages, people have been using human traits (biometrics) to identify others. For example, it is possible to identify a friend by recognising their known faces or voices. Consequently, from various aspects, many new studies reported the importance of using biometrics in our daily life and many definitions have been suggested to give a scientific and specific description. Their high level of uniqueness to a different individual has been adopted for identifying and authenticating users accessing environments that require high security, such as governments, borders and military. It has been tens of years of intensive studies and development of biometric authentication approaches, however, the last decade has seen continuous evolution in this area, covering various daily typical applications and devices including but not limited to: webcams, keyboards, mice, and microphones. Moreover, it is utilised to recognise a person among others inside monitored environments such as searching for wanted criminals among thousands of people across a city (e.g. face, voice or gait recognition).

Bill Gates, declared: “Biometric technologies, those that use voice, will be one of the most important IT innovations of the next several years” (Babich, 2012). It is a science that depends on human’s physiological or behavioural features in order to identify him/her (Jain et al., 2008). Whilst many definitions exist, they tend to focus on similar aspects, such as the

automated method of identifying or verifying an individual. With some also highlighting the different fundamental approaches of physiological and behavioural. For example:

> *"A general term used alternatively to describe a characteristic or as a process. As a characteristic [biometric refer to] a measurable biometrical (anatomical and physiological) and behavioural characteristic that can be used for automated recognition. As a process [biometrics refer to] automated methods of recognising an individual based upon measurable biological (anatomical and physiological) and behavioural characteristic".*
>
> (NSTC, 2014)

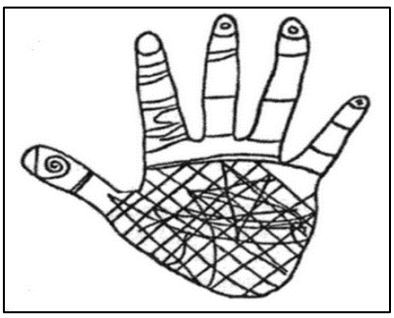
To better understand the mechanisms of human biometric identifiers and its applications in the daily life, almost all studies have classified the biometric characteristics into two distinct types namely: physiological (traits related to people physical appearance, e.g. fingerprint recognition or face recognition) and behavioural (refers to the way people behave, e.g. voice recognition or mouse dynamics) characteristics.

3.2 Biometric Systems

3.2.1 History of Biometrics

The word biometric, originally, is a combination of the Greek words (bio) which means life and (metrics) which means measures (McMahon, 2005). But, no one can claim for sure where and when biometric authentication has been used for the first time in the history. The oldest evidence of using biometric characteristics in the history belongs to 500 B.C. when people of Babylonian civilisation used the fingerprint on clay to indicate the personality in commercial contracts (NSTC, 2006a). Moreover, throughout the history, there was a rich record of using biometrics in the civilisation of Egyptians and the Chinese (Biometric Security, 2014). The popular and well known ancient Egyptian merchants have differentiated themselves from any new merchant to the marketplace through the use of their physical descriptors (Biometric Security, 2014) (Figure 3.1 illustrates the early Egyptian traders were identified by their physical descriptors). About 700 years ago, Chinese merchants utilised biometric authentication in their commercial dealings. As well as the families in that time were used the child fingerprints and footprints to recognise their children from others'

children, interestingly, this simple ink and paper based biometric authentication method is widely used till now (Babich, 2012).



Source: Biometric Security, 2014

Figure 3.1: The Early Egyptian Traders Were Identified by their Physical Descriptors

The early 2000s has experienced significant advances in biometric technologies. In 2000 many events took place, including the introduction of the Face Recognition Vendor Test (FRVT) by the US Government (NIST, 2014b), and the first publication of vascular patterns (Im et al., 2000). Two years later, 2002 was the formation of a standards committee on biometrics ISO/IEC. In the year 2003 was the Official US Government coordination of biometric activities and the establishment of European Biometrics Forum. The Face Recognition Gr NSTC and Challenge (FRGC) begun in 2004 (NIST, 2014a). The markets also got the chance to use their own algorithms for iris recognition when the US patent for the iris recognition concept expired in 2005.

In 2012, the IAI held the world's largest annual meeting of fingerprint experts. The same year saw the creation of the repository of INTERPOL's Automated Fingerprint Identification System (AFIS) which had over 150,000 sets of fingerprints for significant international criminal records from 190 countries around the world. In the begging of 2014, more than 120 million individuals' fingerprints have stored in the largest AFIS database in America which managed by the Department of Homeland Security's US Visit Program. Furthermore, over 200 million fingerprint, face and iris biometric records stored in the world’s largest database (the Unique Identification Authority of India) (Sourcebook, 2014).

3.2.2 Biometric Standards

Given that there are specific kinds of data collectors (sensors/readers) and algorithms for each biometric modality (each is possibly developed by different vendors), it is obvious that implementing multibiometric approach (e.g. multimodal and multi-algorithmic) is apparently

complicated. For such approaches to exist in a vendor- and modality-independent manner, agreed upon standards are crucial to be developed and conformed with. Usually, having several biometric each uses different structure metrics and data format would lead to individuals being locked-in with a particular vendor irrespective of the diversity of performance and cost afforded (NSTC, 2011b). Irrespective

The standards of biometrics have been developed internationally regarding specific modality or the entire biometric system, allowing interoperability between different systems thus, for instance, identifying consolidated biometric data interchange formats. Interoperability is a key aspect for implementing multiple biometric approaches, such as images collected by one device need to be compatible with those collected by another device. Moreover, it must be possible that both of these collected images are interpreted by a third provider product.

International Standards Organisation (ISO) and International Electrotechnical Commission (IEC) have developed main standards supporting the generic goals of biometric standards: interoperability and data interchange among applications and systems. ISO and IEC under Joint Technical Committee 1 (JTC1) Subcommittee 37 (SC37) define that the key aspects covered by these standards are (Podio, 2011; JTC 1/SC 37, 2013):

- common file frameworks (ISO/IEC 19785);
- biometric application programming interfaces (BioAPI) (ISO/IEC 19784);
- biometric data interchange formats (ISO/IEC 19794);
- related biometric profiles (ISO/IEC 24713);
- methodologies for performance testing and reporting (ISO/IEC 19795); and
- cross jurisdictional and societal aspects (ISO/IEC 24779).

Deploying ISO standards such as ISO 19794, 19785, 19784 might avail combining any chosen biometric methods – particular devices will not be able to accomplish this because of the very high costs and processing requirements (ISO, 2006a, b, 2011).

In order to promote interoperability of multiple biometrics-based devices applications and systems, the Common Biometric Exchange Formats Framework (CBEFF) standard (the fundamental standard in the field) has been developed by national and international standards development bodies (InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1 – Biometrics and ISO/IEC Joint Technical Committee 1

(JTC 1) Subcommittee SC 37 – Biometrics) (NIST, 2008), thus, enabling the exchange of biometric information efficiently between system components (NSTC, 2011b).

3.2.3 Biometric Requirements

Each biometric has its strengths and weaknesses and therefore several factors should be taken into account when selecting a particular biometric for use within a specific application. The appropriateness of the potential biometric authentication technique is determined based on the availability of the following seven requirements on the associated trait (Jain et al., 1999):

- Universality
- Uniqueness
- Permanence
- Measurability
- Performance
- Acceptability
- Circumvention

Universality means that each individual uses the application should have the chosen biometric feature, for instance, if all users have hands, it would be possible to use hand geometry as biometric technique. Uniqueness, to differentiate each person from one another, the given trait should be appropriately different for persons in the relevant population. Thereby, more distinctive features will permit more successful discrimination of an individual from a larger population than methods with less uniqueness. For example, whilst face trait would be suitable for accessing a smartphone, accessing military information requires a more unique trait such as iris. Permanence, the biometric trait of any person should be sufficiently stable over the time, as the more the frequent changing of a trait, the more the need to update the biometric template and hence the cost of maintenance (Clarke, 2011). For instance, whereas individual retina scan remains invariant, their keystroke behaviour varies due to device, mode, and text familiarity. Measurability, or the ease of acquisition and digitalization of a particular biometric trait utilising convenience and suitable devices, as well as the ease of extraction of the feature set from the raw trait. Collecting some biometrics is very intrusive – it requires specialised devices and/or explicit user interaction, such as the retina. Conversely, others can be collected easily with normal daily devices and interactions, such as capturing face samples while interacting with the computer. Performance refers to the accuracy and scalability of the technologies required to acquire the feature's samples should be considered with their applications and constraints. Acceptability means the end-users of an

adopted biometrics should be willing to provide their traits and utilise the technique, in terms of, for instance, privacy and convenience. Otherwise, they would resist or avoid using it. Circumvention means how easy it is to duplicate the feature using an artefact or fake alternative, for instance, iris scan is almost impossible to imitate, unlike silicon fingerprints or a photograph of a person (Clarke, 2011).

It can be deduced that a perfect biometric trait to be deployed in an authentication system should meet all the above-mentioned requirements. Nevertheless, there is no biometric currently and highly likely in the future will meet all the above seven characteristics precisely (Jain et al., 2008). Therefore, some studies have suggested the use of multimodal approaches to increase the difficulty of simultaneously forging multibiometrics (Ceccarelli et al., 2014; Ojala et al., 2008; Sim et al., 2007).

3.2.4 Verification and Identification

It is noteworthy to highlight that there are two modes that a biometric system can operate in, namely: verification and identification (Nanavati et al., 2002).

- Verification: seeks to verify that a claimed identity is matched with that on the database.
- Identification: seeks to determine whether the identity exists on the database.

From classification perspective, verification is simpler than identification Clarke (2011). During verification mode the matching process is between sample(s) of claimed individual and the stored template of that individual; thus it is a one-to-one (1:1) comparison. While the comparison is one-to-many (1:N) in identification mode; anonymous sample(s) is compared with every stored template to decide whether there is a match. This means that there is a possibility that the user's template does not exist at all in the database. Hence, the result of the former mode confirms that claimed identity is true or false while the latter decides whether the user is identified or not.

Both these two different modes rely on the application context; if the individual has claimed having enrolled in the system by providing an identity, for example, a username or token with a biometrics, the former mode operates, otherwise the latter does so (Vallabhu and Satyanarayana, 2012). Furthermore, other aspects should be considered when deploying either of the two modes – they are different regarding performance and privacy (Clarke,

2011; Nanavati et al., 2002) as well as cost and user-friendliness. Additionally, due to the involvement of more complexity and computation, identification process typically needs longer time. Consequently, identification needs higher level of system's accuracy and trait's uniqueness than verification.

3.2.5 Components of Biometric System

The biometric process consists five components that can be classified into (Clarke, 2011; NSTC, 2006c):

- Capture
- Extraction
- Template Database
- Classification
- Decision

Sample capturing (acquisition), is the stage of obtaining the biometric samples from the person using some form of sensor depending upon the biometric system, such as optical finger scanner for fingerprint recognition, a microphone for voice recognition, or a web camera for facial recognition. In feature extraction (processing) stage, deploying particular algorithms, the unique characteristics of the captured sample(s) are processed aiming at generating a feature extraction template. For example, in facial recognition, after an image sample is captured, a number of algorithms are performed to extract its distinctive features, such as the distance between the eyes and nose, areas around cheekbones and the sides of the mouth, to create the template. The output of the extraction phase is called a feature vector. The template database is not the raw biometric sample but the template resulted from the aforementioned feature extraction process is stored in a database perhaps along with other user's information. This stored template is utilised as a reference in the matching process afterwards. Therefore, the user enrolment process is completed by the end of the third step. Within identification systems, the fast searching and indexing of the database should be managed effectively in the more complex storage component of the identification system comparing to the verification system, due to the need to search through large volumes of templates (e.g. AFIS has over 150,000 sets of fingerprints). The fourth component is the classification (matching) phase, when a person attempts to have access by providing current biometric samples, the features of these samples are extracted and subsequently compared to

the stored reference template(s) (resulted from the enrolment process) using a matching algorithm. Accordingly, a match score is given representing their degree of similarity, based upon which the authentication decision is followed. Finally, in the decision stage, a comparison between the matching score and the set threshold is performed – if the former equals or exceeds the latter, the access is approved; otherwise, access is denied/rejected or restricted. Therefore, it is also vital to ensure capturing high-quality samples in the enrolment process, because the low-quality samples might lead to errors and misclassification error in the verification process of the legitimate user, or even authorising the wrong person into the system. The whole previous stages are illustrated in the following Figure 3.2.

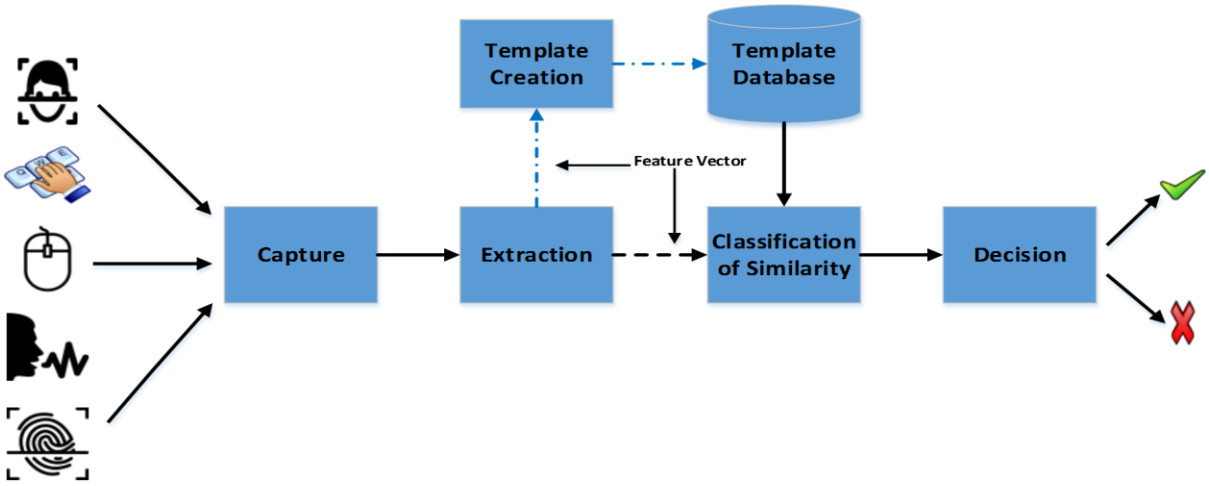


Figure 3.2: The Biometric Process

3.2.6 Biometric Performance

While the traditional authentication methods such as the token-based (e.g. ID card, RFID) and Knowledge-based (e.g. password or PIN) are the only methods that could give a 100% or 0% match between the stored data in the database and the data that has been used for accessing the system in case of validating a person's identity, it is a rare situation to get a perfect match between two of an individual's biometric trait (Jain et al., 2008). This imperfect matching is caused by a variety of factors, including the sensing conditions, changes in the individual's biometric characteristics (behavioural or physiological), alteration in the surrounding environment, or variations in the person's interaction with the biometric characteristic collection device (Nanavati et al., 2002). In biometric based systems, it is interesting to say that a repeated perfect match between two feature sets could give a sign of a potential attack is being launched against this system. As in reality, it is extremely difficult to

repeat the exact circumstances (e.g. positioning, illumination or noise) during collecting data in two consequence data collection processes.

In a verification system, the misclassification of both the authorised user and imposters result in a characteristic error plot between the two main errors. The False Acceptance Rate or False Match Rate (FAR or FMR) is the error associated with the rate at which an imposter is incorrectly accepted by the system, and the False Rejection Rate or False Non-match Rate (FRR or FNMR) is the rate at which the authorised user is wrongly rejected by the system. Obviously, there is a mutual exclusive relationship between these two error rates. Based on the pre-set threshold, which controls the acceptable level of each metric, the security of a biometric system and a users' convenience can be controlled (as illustrated in Figure 3.3). If the threshold is set tighter (i.e. requiring a high matching level), it may yield to genuine users being denied access (i.e. FRR), thus increasing the protection thereby reducing the possibility of illegal users obtaining access (i.e. FAR). Accordingly, authorised users might bother from repeated authentication failure – hence obstructing the adoption of such system. Conversely, if the threshold is set more relaxed (i.e. requiring a low matching level), it maximises the protection of illegitimate users being accepted (i.e. FAR). Despite the fact that this tends to offer a more convenient authentication process to legitimate users by minimising the likelihood of being rejected (i.e. FRR), it would be at the expense of robustness of security. Therefore, it is evident that a balance between system security robustness and user convenience should be considered precisely. A third error rate that is also illustrated in the same Figure 3.3, the point at which both FAR and FRR are equal (i.e. where FAR curve intersects with FRR curve), is called "Equal Error Rate" (EER) (Stanić, 2013; Clarke and Furnell, 2005; Jain et al., 2008; Nanavati et al., 2002). Therefore, it is perceived that the lower EER, the better the overall performance of a biometric system. Nevertheless, the desirable EER would be sought based on users and applications needs and abilities and tolerance slack to both types of errors. For example, increased FRR might be bearable in accessing financial accounts in exchange for securing them by having reduced FAR.

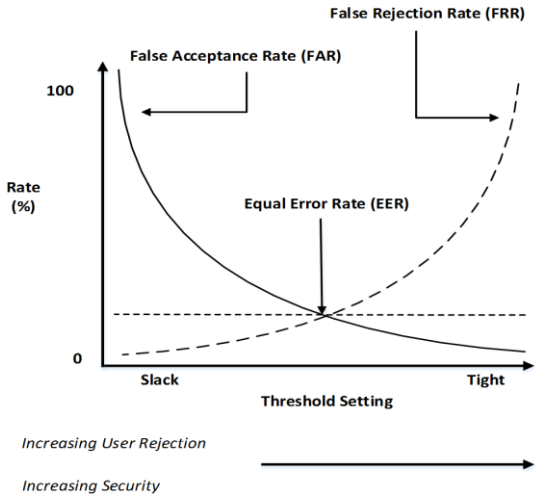


Figure 3.3: Biometric Performance Characteristics FAR, FRR and EER

The FAR and FRR metrics refer to overall system performance of the biometric. These rates are also accompanied by the True Accept Rate (TAR) and the True Reject Rate (TRR) (Clarke, 2011). A report about biometric metrics prepared for the U.S. Military Academy (USMA) defined these two rates as following: "TAR describes the probability that the system correctly matches a genuine user to the corresponding template stored within the system", and "TRR describes the probability that the system correctly denies an imposter, not matching the imposter data to any template within the system" (USMA, 2012).

3.3 Biometric Modalities

As stated previously, based upon the nature of the deployed discriminative trait, studies have classified biometric techniques into: physiological and behavioural. According to the results of the Biometrics Institute Industry 2013 Survey, the former category are more established than the latter and have the biggest user adoption to date. For instance, the survey revealed that the order of which biometrics the respondents are involved in begins with fingerprint, face, iris, multimodal (i.e. more than one biometric modality in one system), and finally speaker recognition (Biometrics Institute, 2013). Notably, speaker recognition is the only behavioural biometrics of the list and it is at its end.

3.3.1 Physiological Modalities

These methods aim at differentiating an individual based upon particular physical characteristics. Given that the stability and reliability of them, many systems rely on them for both identification and verification (NSTC, 2006c). Brief descriptions have been associated with the most well-known physiological biometrics are shown in the following Table 3.1:

Modality	Description
Fingerprint recognition (Jain et al., 2008)	The patterns on the uneven surface of tip of a finger, namely: ridges and valleys
Facial recognition (Jain et al., 2008)	Identify a specific individual in a digital image (the distance between the eyes and nose, areas around cheekbones and the sides of the mouth)
Facial Thermal recognition (Jain et al., 2008)	Identify a specific individual in a thermal image of the face
Ear geometry recognition (Rosen & Carr, 2013)	Base on the height of the ear, reference line cut point and corresponding angles
Iris recognition (NSTC, 2006a)	The coloured tissue between the pupil and the sclera (surrounding the pupil)
Retina recognition (NSTC, 2006a)	The unique patterns on an individual's retina (back of the eye) blood vessels
Palm-prints recognition (Kumar & Zhang, 2005)	The area between the wrist and fingers
Hand geometry recognition (Kumar et al., 2006; Kumar et al., 2004)	The length, width, thickness, and surface area of a person's hand
Sweat pores recognition (Herschel, 2006; Jain et al., 2008)	Very small circular-like structures on the ridges of the fingertip
Wrist/hand vein patterns recognition (Recognition & Authentication, 2006)	The subcutaneous (beneath the skin) vein patterns in a person's hand
DNA analysis (Rabuzin & Sajko, 2006; Clarke, 2011)	The map of human cells, could be the most exact form of individual identification
Brain Wave Pattern (Nakanishi et al., 2012)	Generated by activities of neurons in the cerebral cortex
Electrocardiogram (ECG) (Bonissi et al., 2013)	The heart's rhythm and electrical activity
Electroencephalogram (EEG) (USMA, 2012; Al-Hudhud et al. 2014)	Monitoring method to record electrical activity of the brain
Phonocardiogram (PEG) (Bonissi et al., 2013)	Recording of the sounds and murmurs made by the heart
Photoplethysmogram (PPG) (Bonissi et al., 2013)	A volumetric measurement of an organ
Footprint recognition (Crawford, 2012)	The impressions or images left behind by a person walking or running
Body odour (Babich, 2012; Clarke, 2011)	Caused by skin glands excretions and bacterial activity
Sclera recognition (Sudarvizhi & Sumathi, 2013)	The blood vessel structure of the sclera

Table 3.1: Physiological Characteristics

Due to the stability and reliability of human physiological biometrics, for securing e-assessments, one or more of them can be utilised such as finger, face and iris recognition.

3.3.2 Behavioural Modalities

Behavioural biometrics (as presented in Table 3.2) differentiate people based upon measuring characteristics and pattern of their way of usage (Woodward et al., 2003). Despite the less degree of uniqueness and permanence caused by the erratic nature of these behavioural features because of different reasons, for instance, changing mood, health, and environment, they tend to be more universal, transparent, and hence usable than the physiological ones (Clarke, 2011).

Modality	Description
Signature and handwriting recognition (O'Gorman, 2003)	For instance: velocity along signature path, acceleration, pressure of pen tips, direction of the signature strokes, and time duration of whole signature
Keystrokes recognition (Sulong & Siddiqi, 2009)	The latencies between consecutive keystrokes, hold time of the keystroke finger placement, pressure applied on the keys, and overall typing speed
Mouse dynamic (Sayed and Traore, 2013)	Mouse-move, drag-and-drop, point-and-click, and silence
Keyboard sounds (Roth et al., 2013)	The sound of a user typing on the keyboard
Voice recognition* (Shaver and Acken, 2010; Fant, 2006)	The process of the verification of the identity of the person who is speaking
Gait recognition (Babich, 2012; Subcommittee, 2006)	Discriminating people according to the patterns associated with their walking stride
Gesture recognition (Lai et al., 2012; Sae-bae et al., 2014)	Body, hand, or head movements
Lip motion recognition (Zafeiriou, 2011)	The dynamics of changes of visual features extracted from the mouth region
Hand grip recognition (Chang et al., 2006)	Grasping behaviour, such as how the pressure varying during the grasping process
Behavioural profiling (Li et al., 2011)	The interactions with applications and/or services (which?, when?, and for how long?) of the current technologies such as a personal computer

Table 3.2: Behavioural characteristics

However, some of these features, for instance, a human's voice, contain physiological characteristics such as the physical aspect (vocal tract and mouth), and behavioural characteristics such as the person's accent and his/her behaviour of using of language (Clarke, 2011). Clarke also argued that the classification is depending on the feature itself (how much it plays a role in one of these categories). In 2011, Zafeiriou and Pantic published a paper in which they described facial emotions as a behaviometrics instead of behavioural biometrics, in addition, two years later, (Zhu et al., 2013) referred to behavioural patterns of mobile users as "Mobile Behaviometrics".

3.4 Biometrics in E-Invigilation

This section is divided into two subsections containing two sets of biometric modalities, the first set will be identified based on those that are being used within or have been proposed to be used in the e-invigilation systems, and the second set will discuss additional modalities that could have some role in the future invigilation of e-assessment system.

3.4.1 The Used/Proposed Modalities in E-assessment

Many studies used/proposed biometric techniques in e-assessments, including 3 physiological modalities: fingerprint (Levy and Ramim, 2009; Asha and Chellappan, 2008; Sabbah, 2012; Hernández et al., 2008; Onyesolu et al., 2013), iris recognition (Bal and Acharya, 2011), and face recognition (Irfan et al., 2009). In addition to 4 behavioural modalities including mouse dynamic (Asha & Chellappan, 2008), keystroke analysis (Flior & Kowalski, 2010; Sabbah, 2012), voice recognition (Hayes & Ringwood, 2008), and signature/handwriting (Kikuchi et al., 2008). Therefore, this section will present those biometric techniques in the same previous order.

3.4.1.1 Fingerprint Recognition

In the literature, almost every study that has been written on fingerprint biometrics including but are not limited to (Al-harby et al., 2004; Jain et al., 2008; Ratha and Govindaraju, 2011) highlighted that it is the most well-known, popular, and used biometric technology in the world. This due to its comparatively outstanding features of universality, permanence, individuality, accuracy and low cost. Although the scientific foundation of the modern fingerprint recognition laid by Henry Fauld in 1880 (this means it has been used for identification for more than a century), since about twenty years ago it has become an

automated biometric identification technique (NSTC, 2006d). In an intensive desorption of fingerprint recognition, Maltoni et al., (2009) pointed at the patterns on the uneven surface of tip of a finger, namely: ridges (the high or peaking portion of the friction ridge skin) and valleys (the low, shallow portion of the friction ridge skin) which form a unique fingerprint of each human, and consequently can be used for individual verification of people (see Figure 3.4). Recently, fingerprint identification techniques can be categorised as Minutiae based, Ridge feature based, Correlation based and Gradient based (Mir et al., 2011).

Source: Loyola-González et al, 2015

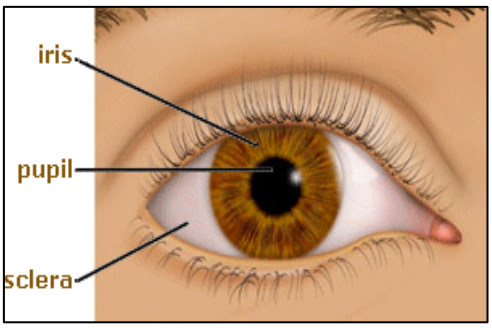
Figure 3.4: An Example of Fingerprint Recognition Showing the Patterns on the Uneven Surface of Tip of a Finger

Although all studies stress on its robustness and uniqueness, fingerprint systems do suffer from many problems, for example, fingerprint placement, dirt and small cut on the finger (Clarke, 2011), noise and distortion during the fingerprint acquisition (Chikkerur & Pankanti, 2006), sensors might endure wear and tear effects over time. This would weaken the performance by increasing the error rates and consequently increase users inconvenience. On the other hand, spoofing attacks (e.g. silicon replicas) were risen as concerns along with the likelihood of stealing fingerprints of people from touched objects or even from distance using a standard camera (Chaos Computer Club, 2014). Yet, present readers are improved by liveness sensor with which some data are collected to decide whether the sample is taken from a living person (Clarke and Furnell, 2005; Maltoni et al., 2009). From a usability point of view, there is a wide deployment of fingerprint recognition in various aspects of life, for instance in securing of laptops or mobile phones (Clarke, 2011). Furthermore, as shown in

Chapter 2, this modality has been utilised/proposed for student authentication in securing e-assessments by five studies; however, the proposal of fingerprint for continuous authentication of students during the e-test is not practical due to the lack of transparency, as the student needs either to touch the fingerprint sensor periodically responding to the system request from time to time or continuously keeps his/her finger on the senor in order to achieve the continuous authentication process.

3.4.1.2 Iris Recognition

The iris is the coloured tissue between the pupil and the sclera (surrounding the pupil) of the human eye (Monitgomery, 2014), which lies between the cornea and the lens as illustrated in Figure 3.5. While the year 1987 saw the first proposal of the automated iris recognition concept (Flom and Ara, 1987), the first suggestion of using the iris patterns as a method to identify a person was in the year 1936 by the ophthalmologist Frank Burch (NSTC, 2006i). In the beginning of the nineties, many working automated iris recognition systems have been developed but the most successful and most popular patented algorithms that can perform iris recognition automatically was implemented by John Daugman in 1994 (Daugman, 1993; Daugman, 2003).



Source: Monitgomery, 2014

Figure 3.5: Anatomy of an Iris

In order to acquire an iris image, either near infrared (NIR) or high-resolution visual light and telescope-type is used. Although a good image of the iris can be acquired by near infrared light without any harm to the individual's eyes (it is a simple illuminated picture of the iris) (NSTC, 2006d), in its emergence, the approach was classified as an intrusive method due to the shortness of the focal length for capturing the image (Clarke, 2011). Nevertheless, Nanavati et al. (2002), reported that one decade later the distances of obtaining images has been increased to reach 40 cm in some desktop-based systems for logical access.

Furthermore, the image of the iris can be taken from a distance of up to 3 metres (Du, 2006). In the other side, the user inconvenience can be caused by the sensation of the cameras to eye alignment (Clarke, 2011). When the iris image is obtained, locating the iris area can be a challenging process as a poorly selected iris area would diminish system performance.

Jain et al., (2008), reported that during the last two decades, iris recognition has widely developed in both the academic and industrial worlds. Recently, the market for iris recognition is growing rapidly (MarketsandMarkets, 2011). Having said that, iris recognition is the third adopted biometric characteristic (Biometrics Institute, 2013). It has been implemented for applications requiring high security. For instance, increasing trillions of iris comparisons (in the stored databases) have been performed around the world since 2001 including iris comparisons of arriving travellers to the United Arab Emirates (MarketsandMarkets, 2014). Furthermore, in the west side of the world, presently, the Iris Recognition Immigration System (IRIS) has been deployed by the UK Border Agency in many airports, such as Heathrow, Gatwick and Birmingham, where monthly, hundreds of thousands of travellers to the United Kingdom have been recognised quickly by simply looking at an iris identification camera without any additional assertion of identity and then pass the barriers within a couple of minutes (UKBA, 2011). Furthermore, borders control has also established since 2011 in both Canada and USA. Many other projects around the world have utilised iris recognition in various domains such as the Aadhaar India's UID project for national identity since 2009, police (i.e. in the USA since 2010), and websites and apps login (e.g. Eyelock device since 2011) (MarketsandMarkets, 2014). Daugman reports a best EER performance of 0.0011 from the NIST Iris Competition Evaluation (ICE) (Clarke, 2011).

Strengths:

1- Iris recognition is a highly robust and stable approach which is ten times more accurate than fingerprint recognition technique (EPIC, 2005).
2- Widely deployed for identification scenarios (Clarke, 2011).
3- The patterns can be imaged from a relatively far distance (Du, 2006). Therefore, comparing with fingerprints technology, iris recognition technique could offer more user convenience and transparent authentication due to the absence of direct contact between the individual and the iris scanner.
4- Highly protected (internal organ of the eye) (Sreekala et al., 2012).

5- The stability: the iris remains stable during the entire individual's life and is not affected by the ageing factor (Sreekala et al., 2012).
6- Safety: The technique uses only safe infrared without any harmful laser. Furthermore, as there is no physical contact with the camera, the iris scan can be performed safely and hygienically (NSTC, 2006a).
7- Speed: It is classified as fast technique (Zhang et al., 2012).

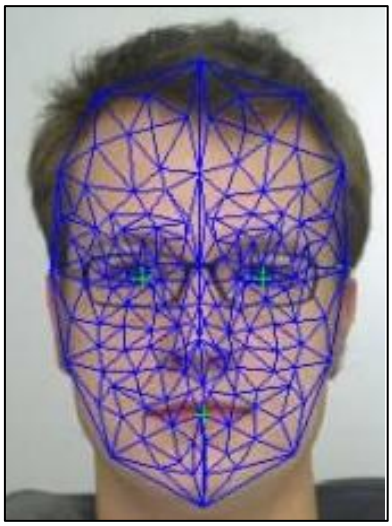
However, the weaknesses can be summarised in the following points:

1- Due to a small target (about 1 cm) to be acquired from a distance (1 m), the system does need individuals to align their eyes with the camera which may cause a certain level of inconvenience (requires user concentration) (Daugman, 2003).
2- Tendency for false rejection (Liu et al., 2013).
3- Due to the importance of the eye for human, some people might feel that the idea of using their iris for authentication purposes is not comfortable.
4- It is not suitable for specific individuals who suffer from eye problems, for instance, blindness and cataracts.

Some other issues might also reduce the performance, such as blinking, eyelashes/eyelids occlusion, movement, and pose from camera (Liu et al., 2013). Therefore, trying to circumvent some of these weaknesses, a number of novel solutions and extraction classifications have been evolved by research aiming at utilising any camera in order to overcome these factors (Daugman, 2007; Roy and Biswas, 2011). For instance, Galbally et al., (2012) proposed utilising a high-quality camera to get the more accurate liveness detection. Multispectral images that require less user collaboration are utilised by Chen et al., (2012) opening the window for employing it in a non-intrusive fashion.

3.4.1.3 Face Recognition

The first effort started to develop the automated system for face recognition was during the 1960s, the purpose of this system was to find specific features on the photographs for instance eyes, ears, nose, and mouth in order to make the required measurements and comparison between the common reference points with the stored reference data for recognising individuals via their facial characteristics (NSTC, 2006f). The following Figure 3.6 presents an example of 2D facial recognition.



Source: Geekosystem, 2011

Figure 3.6: Example of 2D Facial Recognition

Due to the distinctive features of the individual's face and non-intrusiveness (as they can easily be captured without any user interaction), facial recognition has broadly used in computer or access security and crowd observation applications (sometimes the surveillance could occur without person's awareness) (Clarke, 2011; Mir et al., 2011). Although, the universality and acceptability of this method in terms of performance is good in most cases, the method faces some difficulties that could affect the performance of the system such as: the dramatic changes in the facial features of individual's face over long periods of time, the person's weight changes that could occur relatively during short time, bad illumination, position of face, and distance from camera as environmental factors; as well as the effect of long beard, glasses, and hats.

There are some essential features that can be utilised including the distance between the eyes and nose, areas around cheekbones and the sides of the mouth (Clarke, 2011). The FAR and FRR have been approximated to 0.001% and 0.01% respectively by the National Institute of Standard and Technology (NIST) after implementing extensive experiments on the Face Recognition Vendor Test (Phillips, 2007).

Many algorithms have been suggested for face recognition such as: Eigenfaces, Fisherfaces, Independent Component Analysis (ICA), Kernel Principal Component Analysis (KPCA), Kernel Fisher Discriminant Analysis (KFDA), General Discriminant Analysis (GDA), Neural Networks, and Support Vector Machine (SVM) (Matta & Dugelay, 2009). The issue with facial recognition is the range of horizontal movement or angle that the face can be presented

to the camera with most commercial systems operating with +/-20 degree angle, 3D recognition systems, however, offer a far wider range of angles up to 70 degrees (Chang et al., 2010).

Face recognition systems have been developed by many vendors and used for many applications (Face-rec, 2011), starting from full software solutions that process the captured images collected by CCTV cameras to the full-fledged acquisition and processing systems such as cameras and workstations (Nanavati et al., 2002). Facial recognition approaches have been the fastest developing sector among all the biometric techniques (Free-press-release, 2011) with about 5% annual growth in their market since 2010 (MarketsandMarkets, 2011). For example, the (AxxonSoft, 2011) has been proposed to provide face recognition based observation system that can recognise a particular individual amongst a large crowd. The log in process in new Toshiba laptops can be accomplished utilising the features of the user's face instead of typing passwords (Toshiba America Information Systems, 2001). With the rapid growth of mobile computing, facial recognition on smartphone becomes increasingly attractive (Jiawei et al., 2015). Currently, it is an element of many smartphone apps, such as face unlocking, people tagging and games (Yiran et al., 2014).

Strengths:

1- It can be deployed for use as both identification and verification solutions (Jainet al., 2008).
2- It is user-friendly technique because a face photograph can be taken from a distance without any user interaction (Yiran et al., 2014). Therefore, it offers more user convenience due to the absence of direct contact with the camera.
3- Due to the distinctive features of the individual's face and non-intrusiveness capturing, facial recognition has been widely an accepted approach and broadly used in computer or access security and crowd observation applications (Biometrics Institute, 2013).
4- Can be utilised effectively for continuous authentication purposes (Nanavati et al, 2002).
5- The emergence of the new high-resolution 2D and 3D images which mitigates the effects of illumination and face orientation conditions (Chew et al., 2008; Tang et al., 2015).

Having stated all of the above strengths, it is evident that this modality could be considered as the most appropriate modality for providing robust, transparent, and continuous

authentication in e-assessment. Irfan et al., (2009) proposed facial recognition for securing online e-learning systems; however, the study lacks real participant face recognition and ignores the principle of continuous authentication.

Weakness:

1- The major weakness of face recognition methods is that system performance can be affected when a poor quality photo is taken, in which many factors could play important role such as liveness test provisioning (Yu et al., 2014).

2- It is debatable that the human face shape may change over time and so the system template should be updated accordingly if necessary (Chang et al., 2010).

However, in order to mitigate these weaknesses, a number of solutions have been suggested. For instance, when collecting the samples, a number of individual's face images in different sizes, illumination and orientations can together be stored as a template, it will be compared with the stored composite template (Clarke et al., 2008). Nevertheless, due to the sophistication of this approach, the balance between user convenience and the level of security in the system is not an easy process. Furthermore, a more promising solution that involves the three-dimensional camera to provide the depth information, using infrared beams ability, can offer a good alternative to diminish the effects of both face orientation and lighting conditions.

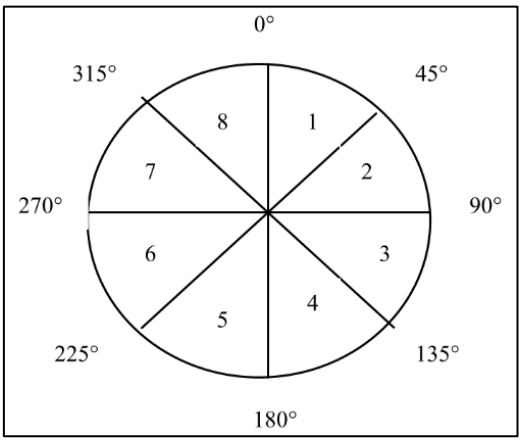
3.4.1.4 Mouse Dynamic Recognition

Mouse dynamics can be defined as the characteristics of the actions received from a computer-based pointing device such as the mouse or a touch-pad for a particular individual while interacting with a specific graphical user interface (Shen et al., 2013; Bours and Fullu, 2009; Feher et al., 2012). Some features can be captured non-intrusively from mouse actions that differ from an individual to another. Mouse actions can be categorised into one of the following (Ahmed and Traore, 2007; Shen et al., 2012):

- Single click: Mouse down event followed by mouse up event of left/right/middle buttons
- Double click: A continuous operation of mouse down, up, down and up event of left/right/middle buttons

- Mouse-Move: General mouse movement involving no clicks
- Point-and-Click: Mouse movement followed by a click or a double click at the end.
- Drag-and-Drop: The action starts with mouse button down, movement, and then mouse button up, and;
- Silence: The standstill of mouse cursor (a situation without any mouse operations).

The considered mouse directions of this system are shown in Figure 3.7.



Source: Asha and Chellappan, 2008

Figure 3.7: Example of Mouse Movement Directions

Generally, as an authentication technique, mouse dynamics hold promising performance. It might provide error rate better or similar to other widely deployed techniques such as speaker recognition (Ahmed and Traore, 2007; Gamboa and Fred, 2004). Nevertheless, they might be over optimistic in their assessment, as there is a limited impractical evaluation in the literature that could support this argument (Jorgensen and Yu, 2011).

Various studies, techniques and usages of mouse dynamics approach have been suggested during the last two decades. In 2003 Everitt and McOwan investigated the likelihood of distinguishing users by the way of their mouse operating styles. Since then many other studies highlighted the ability of utilising mouse dynamic for continuous authentication. In this regard, Pusara and Brodley, (2004) offered a continuous authentication method using mouse movements and mouse events as features. Using Decision Tree Classifier with smoothing filters for classification, they collected data from 11 users on their own personal computers under a free environment. An average FAR of 1.75% and average FRR of 0.43% were reported. Ahmed and Traore, (2007) presented a continuous authentication approach with mouse dynamics. They used fuzzy classification based on the learning algorithm. Using

data from 49 participants, they achieved an FAR of 0% and an FRR of 0.36%. Furthermore, Gamboa and Fred, (2003) proposed mouse movements for continuous authentication, in which every movement was considered as a stroke to capture and extract the characteristics of mouse behaviour. After archiving an experiment involving 50 users under a free environment, they have reported results on 100 strokes (EER of 0.7%).

However, the main observation from the previous discussion is that the issue of behavioural variability of the mouse dynamics biometrics has not been carefully considered (Bours and Barghouthi, 2009). Moreover, similar to the other types of behavioural biometric modalities, mouse dynamic can only be utilised for verification purposes but is not unique enough to be employed for identification solutions. Therefore, it still needs to be combined with other authentication techniques in order to provide satisfactory performances feasible for identification mode.

The key advantage of mouse dynamics biometric technique is its ability to constantly monitor the people based on their sessional usage of a computer system. Having said this, it is evident that the mouse dynamic and all the similar behavioural biometric modalities (e.g. keystroke analysis or speech recognitions) are essential to be involved in combination with other transparent but more robust modalities (e.g. facial recognition) in order to build an efficient multimodal biometric system that can work in continuous and transparent fashion. For instance, for the necessity of continuous authentication of students particularly in case of e-assessments, Asha and Chellappan, (2008) proposed multi-biometric system involving mouse with biometric fingerprint scanner, using this device would enable them to utilise both fingerprint and mouse movements to build a multi-biometric authentication system.

Advantages:

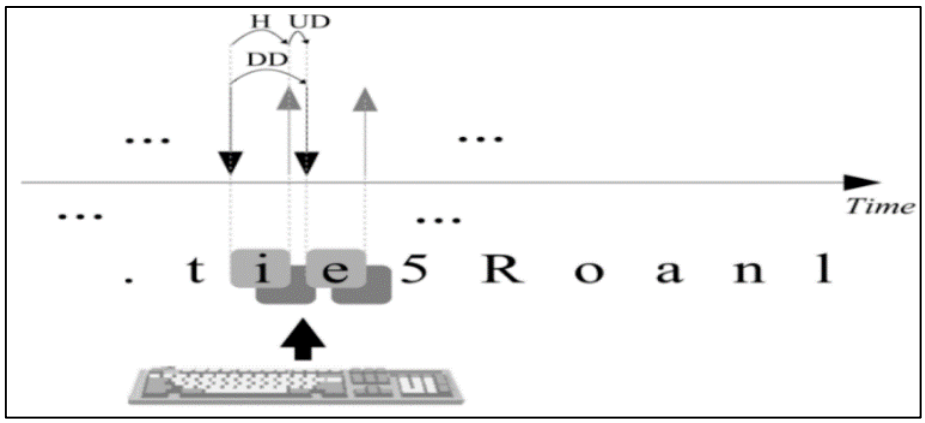
1- It does not require a special or additional hardware device for data collection (Bours and Fullu, 2009).
2- Inexpensive, easy to use, and popular (Feher et al, 2012).
3- Can be utilised effectively for continuous authentication purposes (Sayed and Traore, 2013).

Disadvantages:

1- Mouse dynamics techniques can only be utilised for verification purposes but is not unique enough to be employed for identification solutions (Shen et al., 2012).
2- It requires a long time and effort to create user's template (Sayed and Traore, 2013).
3- It requires changing the templates frequently in order to reach the optimum of current actual individual's mouse usage (Bours and Fullu, 2009).

3.4.1.5 Keystroke Analysis

Keystroke analysis describes the action when an individual interacts with a computer keyboard. It is supposed to verify people based upon their discriminatory typing patterns. Although the speed of typing depends on the mood of an individual and a time of a day, the way of typing differs from one person to another which indicates some unique priorities (Classifiers & Engineering, 2009; Teh et al., 2010). During the early 1980s, a large and growing body of literature regarding the issue of using keystroke dynamics for authentication purpose or to provide additional security was investigated (Gaines et al., 1980; Umphress and Williams, 1985). The authentication process can be achieved based on either a more reliable static (text-dependent) or a dynamic (text-independent) modes (Clarke, 2011). The latencies between consecutive keystrokes (the time between the release of a key and the depression of the following key), and the hold time of the keystroke (the duration that the person holds the key down) (see Figure 3.8), are the main two features among many other person's distinctive typing features while using typical computer keyboard (such as finger placement, pressure applied on the keys, and overall typing speed) that can be used to differentiate between users (Babich, 2012; Karnan et al., 2011; Classifiers & Engineering, 2009; Teh et al., 2010).



Source:(Montalv et al, 2014)

Figure 3.8: An Example of Keystroke Analysis (Visual explanation of Down-Down (DD), Hold (H) and Up-Down (UD) intervals.)

During the last four decades, many authors, in their related studies, have considered keystroke analysis as an effective method to achieve the continuous authentication process of users in which this process is essential for particular systems such as e-assessment monitoring (Flior & Kowalski, 2010; Sabbah, 2012). However, since the 1970s, this technique has not been developed and deployed extensively, except some commercial solutions that incorporate it with other authentication techniques (e.g. password). A recent study explored by Ahmed & Traore (2014) highlighted the principle of dynamic and passive monitoring to provide a continuous authentication based on the free text detection. Furthermore, according to a study accomplished by Joyce and Gupta (1990), a short string has been used to specify FRR of 16.36% with an FAR of 0.25 of the keystroke analysis.

Advantages:

1- Keystroke analysis can offer an additional layer of security to existing password-based access control approach (Newspapers, 2007).
2- Inexpensive, and easy to use (Gunathilake et al., 2013).
3- Keystroke dynamic is a non-intrusive and widely accepted approach (Ferreira and Santos, 2012).
4- It can be utilised effectively for continuous verification of students while they work on such tasks as writing essays, report or long answers during the e-assessments (Bours and Barghouthi, 2009).
5- No further hardware is needed as the technique is embedded within the keyboard system (Saevanee, 2014).

Drawbacks:

1- The main downside of keystroke analysis is that it is like other kinds of behavioural biometric techniques; it can only be utilised for verification purposes but is not unique enough to be employed for identification solutions (Jain et al., 2008).
2- It requires long time and effort to create the reference template of user's typing (Clarke, 2011).
3- It requires changing the templates frequently in order to reach the optimum of current actual person's typing speed (Gaines et al., 2009).
4- There is limited commercial use of this authentication method (Clarke and Mekala, 2007).

3.4.1.6 Speaker Recognition (or Voice Verification)

About 100 separate features of the individual's voice that make speaking biometrics to be as reliable as fingerprint biometrics (Babich, 2012; Hayes & Ringwood, 2009). The first model of explaining the physiological components of acoustic speech production was created by a Swedish professor, Gunnar Fant in 1960 (NSTC, 2006k). There is an occasional confusion between the technology of translating the individual's words - speech recognition, and the process of the verification of the identity of the person who is speaking - speaker verification (Nanavati et al., 2002). The latter technology is based on the analysis of the frequency of the individual's speech sample and its corresponding features (e.g. the quality, period, intensity dynamic, and pitch of the signal), that is compared with the previously processed and stored template in the database (NSTC, 2006k). Trying to explain the speaker recognition, (Clarke, 2011) argued that the speaker or voice verification is the strongest inherited behavioural amongst all other individual's behavioural biometrics with an EER approximately 2%; nevertheless, the nature of the acquired sample plays a role in the viability of the performance features, whereas it utilises the physiological organs such as mouth (oral cavity), nose (nasal cavity) and throat (larynx).

Many studies including (Hayes & Ringwood, 2009; Clarke, 2011) stated that similar to the previous behavioural biometric trait (Keystroke recognition), the speaker authentication process can be achieved base on either a more reliable static (text-dependent) or dynamic (text-independent) modes (Shaver & Acken, 2010; Nanavati et al., 2002; Crawford, 2012; Gao, 2012; Jain et al., 2000), with the former, the individual speaks a predefined phrase or given number(s) whereas the spoken input is free with the latter. Although the static mode provides less user-friendliness, Woodward et al., (2003) said it offers lower error rates.

Since Gunnar Fant founded in 1960 an x-rays based model for the acoustics of speech production (NSTC, 2006h), several studies in this area have been established. The fact of the current widely used telecommunications revolution (mobile phones, telephone landlines, and Voice over IP network or VoIP) around the world has given additional advantage to speaker verification technology over other biometric traits, which opens the door for remote authentication on account of its ease of integration and the large number of distributed speech samples gathering devices such as computer microphones (Jain et al., 2008; NSTC, 2006a). Biometrics Institute, (2013) stated that voice recognition is on the top of the deployed behavioural biometrics and the fifth among all biometrics. Currently, most speaker

verification algorithms can leverage personal computer hardware (i.e. microphone); therefore, this offered the ability to involve speaker recognition techniques for continuous authentication (as the case with other behavioural biometrics discussed formerly) in many existing computer-based security system including the online test authentication systems such as (Hayes & Ringwood, 2008) that mentioned in the literature of this research. Furthermore, in their review of human biometrics or characteristics based authentication that could be utilised in e-assessment solutions, Ullah et al., (2012) stated that the way in which a person speaks (e.g. accent, speed or manner) represent unique features and it can be used in e-examinations to specify a test taker's identity. Therefore, a prototype designed by Hayes and Ringwood (2008) involving voice recognition to provide security in this area. Typically, speaker recognition represents one of the best-performing behavioural approaches with an EER of approximately 2% (Przybocki et al., 2007). Yet, the viability of the performance characteristics in this study depends upon the nature of the sample.

Advantages:

1- It is a non-intrusive and widely accepted approach (NSTC, 2006h).
2- Can efficiently be used with speech recognition and spoken password.

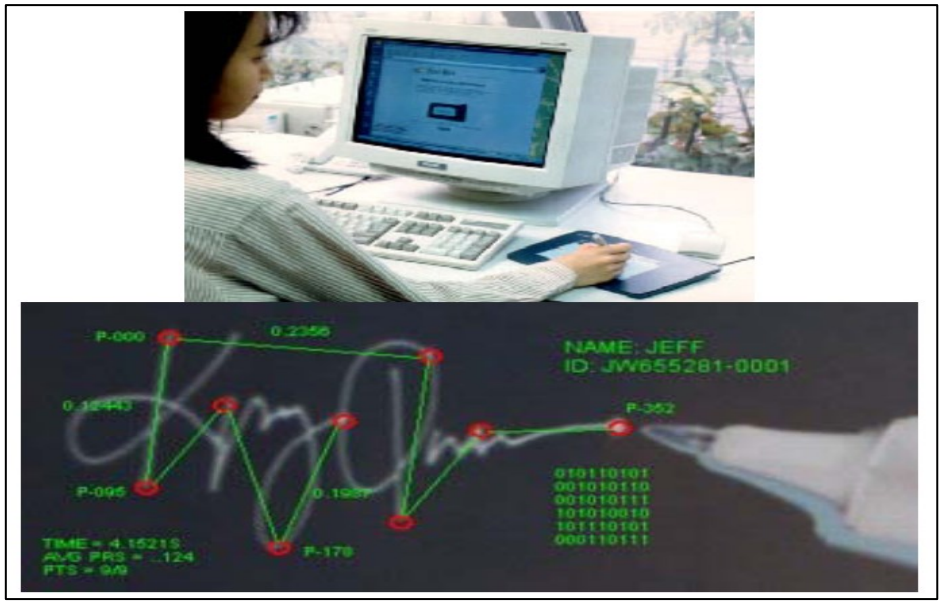
Disadvantages:

1- In a study which was set out to determine speaker recognition error rates, Shaver & Acken, (2010) found that many aspects could play negative role against this technique such as changing talking style, ambient noise, or recording quality.
2- The susceptibility of a bad transmission channel, low-quality voice capturing devices and microphone variability that could represent a real challenge (NSTC, 2006b).
3- A possibility of recorded voice spoofing (Jain et al., 2008).

3.4.1.7 Signature/Handwriting Recognition

The first development of signature recognition system was in 1965, nine years later, in 1974; the work began on signature recognition by the Standford Research Institute and National Physical Laboratory (Babich, 2012). Many distinctive behavioural features of a signature (for instance: speed, pressure and stroke order) are used to verify the identity of the individual in the signature verification scheme.

A considerable amount of literature has been published on signature recognition as one of the first accepted civilian and forensic behavioural biometric verification technique in our societies. These studies have emphasised on the principle of using the anatomic and behavioural characteristics that a person behaves when signing his or her chosen word(s) for recognition purposes (Meshoul & Batouche, 2010; NSTC, 2006d). The signature recognition is relatively a new biometric technology to be utilised with the current contact sensitive technologies such as touch screen interfaces of many new devices including but not limited to mobile phones and digitizing tablets as shown in the following Figure 3.9, where the identity of individuals has been verified based on their signatures on paper.



Source: NSTC, 2006a

Figure 3.9: Dynamic Signature Depiction

The digital handwritten signature authentication has been classified into two main types, namely: static and dynamic (Nanavati et al., 2002). Static authentication is considered the least robust method due to it is suffering from forgery actions and extracts the actual features of a signature from the final image of the signature by simply examining the handwriting appearance, i.e. the curvatures, angles and patterns of letters or symbols and comparing it with the genuine image. Dynamic signature recognition, however, utilises many distinctive behavioural features of a signature which are involved to verify the identity of the individual in the dynamic signature verification schemes, i.e. the velocity along signature path, acceleration, pressure of pen tips, direction of the signature strokes, and time duration of whole signature (Guse, 2011).

Advantages:

1- One of the efficient behavioural biometric approaches. Comparing with other behavioural biometric methods, signature recognition has a better performance rate with an EER of 2.84% (Yeung, 2004).
2- This approach utilises the facilities which are provided by the variety of current contact sensitive technologies (Clarke, 2011).
3- It is considered as one of non-invasive authentication approaches (Nanavati et al., 2002).
4- It provides a degree of flexibility to the individual in which he/she has the chance to change his/her signature (Nanavati et al., 2002).

Disadvantages:

1- It suffers from increased error rates due to variable signatures (Ratha and Govindaraju, 2008).
2- Many persons are unfamiliar to signing on touch screens (Nanavati et al., 2002).
3- It has limited applications (Jain et al., 2008).

This technique can also offer a feasible non-intrusive transparent and continuous authentication by capturing the samples while an individual is writing words on a tablet PC or signing on a point-of-sale terminal, which opens the window for employing it for continuous authentication in e-assessment such as Kikuchi et al., (2008). Clarke and Mekala (2007), empirically proved that the signature recognition could be used for hand writing on mobile-based devices. Despite the small number of subjects, the experiment accomplished a promising performance with 0% FAR and 3.5% FRR in a controlled environment and 0% FAR and 1.2% FRR in a feasibility environment. Nevertheless, in this study, the effect of the written word length has not been highlighted. In general, given the probability of variations in handwriting even if are done successively by the same individual, therefore it is very difficult to forge this method by others. However, it is still sufficient for verification not identification mode.

3.4.2 Modalities Could Have Some Role in Future

This section will discuss additional modalities that could have some role in the future of invigilation of e-assessment systems.

3.4.2.1 Facial Thermogram Recognition

Under the skin of his/her face, each individual has unique veins and tissue structures. For individual identification, the approach depends on an infrared camera to capture a thermal image of the face by sensing the heat pattern caused by the blood flow (Woodward et al., 2003; Socolinsky et al., 2003; Socolinsky & Selinger, 2004). The following Figure 3.10 illustrates a thermal image of the face.

Source: Socolinsky & Selinger, 2004b

Figure 3.10: Automatic Detection of the Face and Eyes Shown on an Overlay of Visible and Thermal Images

Strengths:

1- The stability: It is more stable than the face of the person, and is less affected by short time effects such as person's weight changes, beards, glasses, and hats.
2- Safety: With respect to safety, there is no possibility to harm the individual's eyes during the process because the technique uses only safe infrared without any harmful laser (Jain et al., 2000).
3- These thermal data that can typically be extracted with minimal environment inference and users interaction may enable transparent deployment.
4- In order to acquire the image, it does not require good illumination conditions (Woodward et al., 2003).
5- High level of convenience: Offers more user-friendliness due to the absence of direct contact between the individual and the face thermal scanner. This supports the potential of utilising it within e-assessment authentication as further biometric modality, perhaps coupled with facial recognition, and hence overall authentication performance would improve significantly.

Weaknesses:

1- It cannot be used for identification as its performance is not accurate enough (Socolinsky and Selinger, 2004).
2- Due to the importance of the eye for human, some people may feel discomfort (do not prefer) with the idea of projecting infrared beams to capture a thermal image of the face by sensing the heat pattern caused by the blood flow.

3.4.2.2 Ear Geometry Recognition

The various small valleys and hills which furrow across the human's ear (including the distinguishing features: helix, lobe, and concha (Ross, 2011)) have been considered by Alphonse Bertillon since 1890 to be potential features for individual identification (Jain et al., 2008), yet it has not been experimentally validated until Iannarelli developed his scheme in 1989 (Arbab-Zavar and Nixon, 2011). More recent studies are trying to utilise the high level of non-intrusiveness that this method can provide, for instance, Fahmi et al, (2012) proposed implicit authentication through images of the user's ear employing the smartphone camera during a call. Experimentally, under specific conditions research has stated recognition rates between 93% and 99.6% (Moreno and Sanchez, 1999; Hurley et al., 2005).

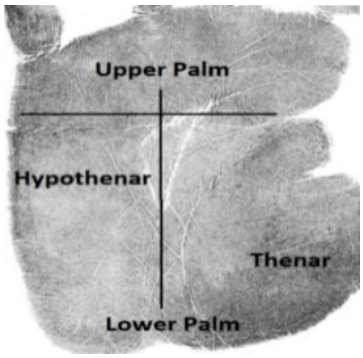
Advantages:

1- The camera can easily capture the ear from a relatively far distance (Abaza et al., 2013).
2- The ear characteristics, throughout the individual's life, are relatively stable comparing with many other biometric techniques such as the face that have obvious effects of ageing (Wu, 2011).
3- Cummings et al., (2010) accomplished 99.6% success rate, therefore, ear geometry can be employed for both identification and verification.
4- They are not impacted by surrounding environment (e.g. illumination), apart from varying angles and hair and earrings occlusion which can be controlled and normalised (Arbab-Zavar and Nixon, 2011).
5- Can be utilised for transparent user authentication, for instance, in the e-assessment environment, when the student turns his/her face left/right the camera could capture the ear image even without his/her knowledge as they can be recognised clearly from distance.

Although the above advantages and high accuracy, there is no commercial ear geometry product (Clarke, 2011; Ross, 2011).

3.4.2.3 Palm Print

Palm print is the area between the wrist and fingers, as shown in Figure 3.11. The first recorded methodical capture of hand and finger images were used by Sir William Herschel in 1858 to differentiate between employees. It has not evolved to be automated until 1994 in Hungary (Woodward, Orlans and Higgins, 2003). In an analysis of Palm print features, Shu & Zhang (1998) stated features include ridges, singular points, minutia points, principal lines, wrinkles and texture.



Source: Wikimedia Commons, 2014 (Modified)

Figure 3.11: Palm Print

The palm print verification systems have been classified into two types, namely, high-resolution systems which are based upon high-resolution images (utilising specific features including ridges, singular points and minutia points), and low-resolution system which employ low-resolution images (utilising specific features including principal lines, wrinkles and texture). Other studies have indicated that there are four categories of palm print verification techniques namely: line based, texture based, orientation based, and appearance based (Mir et al., 2011). In addition to traditional live-scan approaches, there are various types of sensor which can be used for gathering the digital image of a palm surface such as capacitive, optical, ultrasound, and thermal (NSTC, 2006j). In order to capture the individual's palm image, some of these systems, to gain a better performance, divide the palm into relatively small parts; others scan the whole palm region (Kong et al., 2006). Many palm print recognition systems have been developed and adopted within the commercial and state utilisation (NSTC, 2006g). It also embedded into the FBI's Integrated Automated Fingerprint

Identification system (IAFIS) and consequently their recent Next Generation Identification system (NGI) in which palm print ability added to it (NSTC, 2011b).

Advantages:

1- Its image can be collected using low-resolution devices (Kong et al., 2006).
2- It can be used for identification and verification modes (NSTC, 2011b).
3- Palm print recognition is considered as one of the most acceptable methods among available biometric methods (Shu and Zhang, 1998).
4- Comparing with other biometric recognition methods such as iris recognition, many people are more comfortable to use palm print recognition due to it will not cause damage to the sensitive organs (Jain et al., 2008).

Palm print recognition systems have some shortcomings exceeding those of fingerprint techniques; for example, the large capturing machine, the relatively larger template size compared to fingerprint, and the possibility of palms geometry features to change as a result of ageing or weight (Nanavati et al., 2002). However, because it works in a similar manner as the fingerprint works (fingerprint proposed by many studies for securing e-assessment), this modality could be used to add a level of security in the beginning of the e-test but it would not provide transparent authentication as the face for instance do.

3.4.2.4 Behavioural Profiling

The growing use of computers in recent decades has led to the emergence of a new method of behavioural biometric, called behavioural profiling. It is one of the most non-intrusive approaches for individual authentication utilising his/her interactions with applications and/or services (which?, when?, and for how long?) of the current contact technologies such as a personal computer (Aupy and Clarke, 2005). The historical behavioural interactions of the individual are used to create a profile template to be utilised at the authentication process whilst the usual user's interaction to decide whether it is the legitimate user identity or vice versa when the usage pattern deviates.

It has been investigated taking various aspects into consideration, including network-based, device/host-based, desktop or mobile environments, and deploying it alone or combined with other authentication techniques (Aupy and Clarke, 2005; Li et al, 2011; Saevanee et al.,

2012). In 2012, Li proposed this approach for preventing any unauthorised access to mobile devices.

Advantages:

1- It offers sufficient distinctive features to verify a user transparently and continuously (Li et al, 2013).
2- From the users' convenience point of the view, behavioural profiling is considered as one of the most user-friendly approaches. It monitors behavioural patterns on most kinds of devices without any interruption, which makes it further good approach for transparent and continuous authentication (Li, 2012).
3- It has been proven that individual recognition rates above 90% with no more 3% as false alarm rates (Saevanee et al., 2012).

Therefore, from the above evidence, behavioural profiling modality could be utilised in future for adding a level of security in the transparent and continuous authentication of e-assessment.

Disadvantages:

1- The main drawback of this method is the continuous changing in the person's reference template (Saevanee et al., 2012).
2- Behavioural profiling cannot be used within an identification system as it is not unique and distinct enough technique. It is probably more feasible to be incorporated with a multi factor/biometric authentication system.
3- Lack of users' privacy, due to the continuous monitoring of the uses, some of their private information such as passwords, could be exposed to misuse by others. Thus, fearing from the seepage of private information that might happen during the behavioural profiling proctoring would affect the level of user acceptance (Aupy and Clarke, 2005).

To date, there is a rare use of this technique by the authentication mechanisms thus far. In the literature, to best of the author knowledge, the closest study to the idea of behavioural profiling of the students (profile based authentication framework or PBAF for short) together with a user-id and password for the authentication purposes during online examinations was suggested by (Ullah et al., 2012). On the other hand, currently, this technique is being used

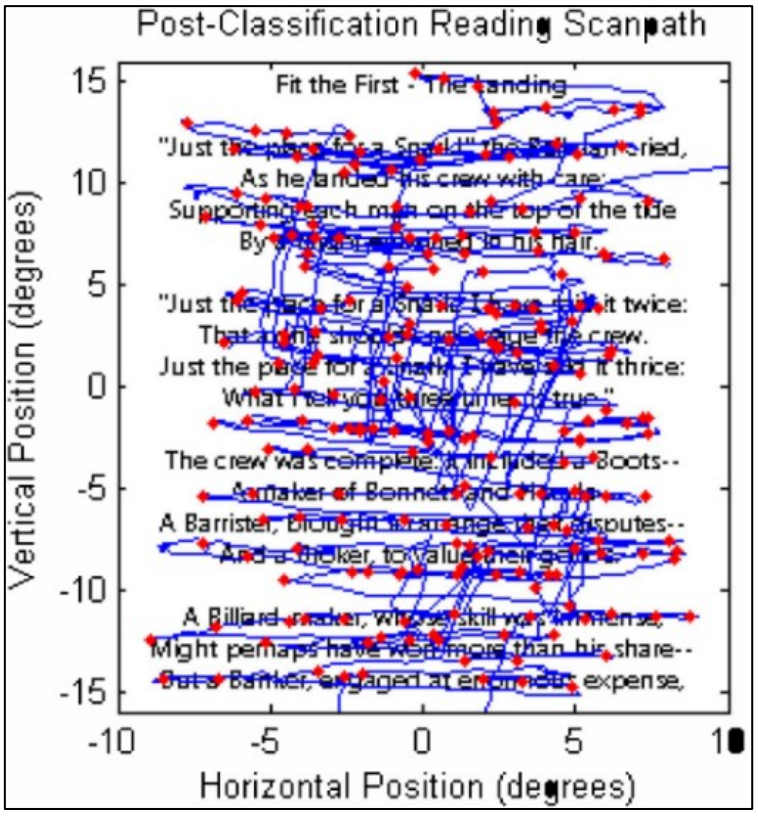
by many companies for credit card and mobile telephony systems protection against any potential fraud actions (Gosset, 1998; Stolfo et al., 2000).

3.4.2.5 New Promising Biometric Modalities

There is no doubt that student's head (including face and eyes) is the most interactive/communicative organ with the computer during the e-assessment, opening the door for employing further relatively new behavioural biometrics, namely: eye and head movements, that have not been employed in this area and can offer a promising solution.

3.4.2.5.1 Eye Movements

In addition to several physiological measures provided by the human eye such as iris and retina patterns, eye movements could offer a robust behavioural biometric (Saeed, 2015). The idea of employing patterns obtained from eye movements for biometric recognition is relatively new and a growing field of research. It relies on both behavioural (brain) and physiological (muscles) features of the individual. These movements can be collected using eye tracking devices. Most of the current eye trackers use video image analysis or invisible near infrared light emitters without any harm to the individual's eyes (Pawe Kasprowski and Ober, 2004). This gives the ability to capture an exact point an individual is looking at in a given moment of time (it is called fixation which lasts for about 200-300 milliseconds – during fixations the eye is almost still). Then, during the time of observing a user's eyes, a relatively large number of consecutive fixations are collected quickly. In addition to fixation, the eye globe rotates quickly between points of fixation with very little visual acuity maintained during rotation creating what are called saccades (Holland, 2012). Both fixation and saccades are mainly produced by the brain and represent the information required to produce the discriminative features of eye movement biometrics. The merge between fixation and saccade data of a user's reading scan-path is demonstrated in Figure 3.12. Fortunately, eye tracking has now developed to the point where the individual can move almost freely in front of the camera (Porta et al., 2012).



Source: Holland and Komogortsev, 2011

Figure 3.12: Example Reading Scan-Path

The first study explored eye movement features in the field of biometrics were offered in 2004 by (Kasprowski and Ober, 2004). They used Cepstrum transform in order to examine the uniqueness of the characteristics that might be enclosed into the spectral components of eye movements. 1% FAR and 23% FRR were reported as the results for a database of 9 subjects. Since then, many attempts have been achieved by researchers to improve the performance involving different experiments. The most recent empirical research has been presented by (Rigas and Komogortsev, 2014). They suggested a method called fixation density map (FDM) to extract biometric features from the spatial patterns formed by eye movements throughout an observation of dynamic visual stimulus. They claimed that they achieved significant improvement over existing approaches, the eye movements collected from 200 users provided an EER of 10.8%. However, so far, to best of the author knowledge, eye movement techniques have not been employed for securing e-assessment within the e-learning environment.

Strengths:

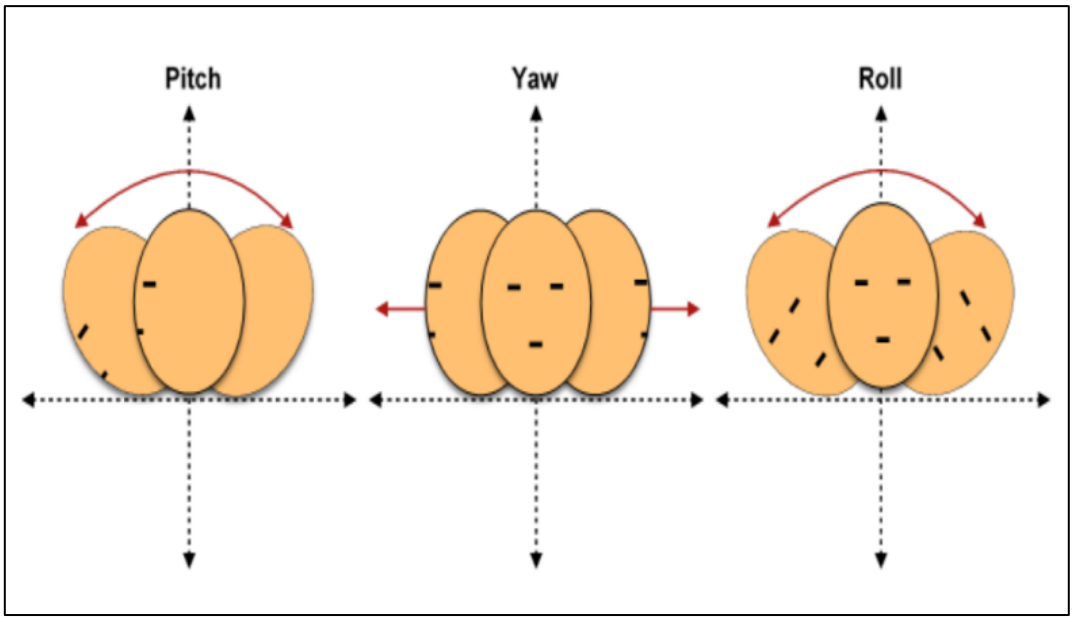
1- Can be utilised effectively for non-intrusive and continuous authentication purposes (Rigas and Komogortsev, 2014).
2- Eye movements can be collected even without user cooperation that offers a covert or passive identification using hidden cameras (Porta et al, 2012).
3- It seems impossible to mimic or forge eye movements due to the fact it is mainly created and controlled by the brain.
4- Although it has been suggested as a soft biometrics (secondary), research proved a high level of accuracy achieved. This opens the door to use it as a primary biometric modality.
5- Many inexpensive and accurate eye trackers with efficient Software Development Kit (SDK) have currently become available.
6- Eye movements can be recorded and processed effectively using new 3D cameras.

Weaknesses:

1- Some people might feel that the idea of using their eyes for authentication purposes is not comfortable.
2- It is not suitable for specific individuals who suffer from eye problems, e.g. blindness and cataracts.

3.4.2.5.2 **Head Movements**

Biometrics using patterns obtained from head movements can be considered as the newest field of research. Head movements could offer a source of biological uniqueness, since it is naturally known to be affected by both posture and slight anatomical differences between people, for instance, the physiology of neck muscles (Rogers et al., 2015). Head movements can be collected using 3D web camera which can continuously measure the depth of the scene via infrared light, and then collect the three main head movements namely pitch, yaw, and roll (see Figure 3.13), that form cornerstone for building the recognition system. The measurement values can be a treasure of data (about 75 (3X25) samples every second). In relation to head movement, a pitch is when the head nods; a yaw relates to the axis that a person shakes their head on; and a roll is when the head leans to either side.



Source: Rogers et al, 2015

Figure 3.13: Pitch, Yaw, and Roll in Terms of Head Movement

Generally, head movements appear as a potentially precious source of characteristics considering the present trend for convenient touchless appliances, capable of interacting with face region (Rogers et al., 2015). Obviously, the student's head/face is the most interacting organ during the e-test, having said this; it is evident that head movement data is another biometric that is capable of being utilised for transparent and continuous identity verification. Moreover, as the collecting of head movements is accomplished from the head area, extracted features could be combined with other established biometric traits captured from the same region, in order to form multimodal approached based on more classic features, for instance: eye movements, periocular, nose, lip, or blinking biometrical signals.

3.5 Other Types of Biometric

In addition to the above, many other physiological and behavioural biometric approaches have been mentioned/proposed in the literature, however, currently have limited empirical or commercial basis. These include:

1- Facial colour (Sudarvizhi & Sumathi, 2013).
2- Fingernail bed recognition (Kumar et al., 2014).
3- Foot dynamics (Jung et al., 2003).
4- Colour of the clothing (Sudarvizhi & Sumathi, 2013).
5- Acoustic Ear Recognition (Clarke, 2011).

6- Skin Reflection (Nanavati et al., 2002).
7- Vascular Pattern (Michael et al., 2012).
8- Dental evidence (Jain et al., 2008).

3.6 Limitations of the Current Biometric Systems in E-assessment

As highlighted in Chapter 2, many researchers have argued that the strategy of using a single biometric has not been successful for candidate authentication in online examinations. Therefore, studies have sought to focus upon multimodal biometric systems. However, in terms of implementations, both methods suffer from many limitations that include:

1- The need for additional equipment or biometric devices: the laboratory equipment may be very costly (Jain et al., 2000), and there is no guarantee that these devices will be kept safe and secure after the completion of a test. Moreover, the high cost of some required equipment makes the system infeasible to be utilised for e-learning examinations purposes (Blinco et al., 2004).
2- Many methods including but not limited to fingerprint suffer from a lack of transparency (non-intrusiveness) (Fadhel et al., 2011).
3- The high possibility of fraud actions, for instance, (Jain et al., 2000; Nanavati et al., 2002; NSTC 2006b; Jain et al., 2008; Clarke, 2011) identified several attacks against biometrics such as a fake fingerprint (Silicon or Jelly fingers) or spoofing facial recognition using photograph (Clarke, 2011). Furthermore, in another study, Eveno & Besacier, (2005) reported that a recorded voice of the candidate can be used instead of the actual live voice for achieving the fraud actions.
4- Many people are concerned about their own sensitive biometric features regarding their security and privacy, especially the physiological biometrics which accompanies the person for his/her entire lifetime and cannot be changed easily as it is perhaps the case with behavioural biometrics (Weaver, 2006; Clarke, 2011).
5- Over the time many human biometrics could change, particularly the behavioural biometrics (e.g. keystroke analysis) (Maltoni et al., 2009).
6- Human body might suffer from the lack or even absence of some physiological biometrics as they become elder such as fingerprint, iris, or retina (Weaver, 2006; Clarke, 2011). Some people have a permanent disability, for instance, accidentally organ losing (USMA, 2012; Crisp, 2011; Alotaibi & Argles, 2011).

7- Privacy: Except the behavioural, all kinds of biometrics are permanent and cannot be changed; therefore, many people might refuse the idea of using such technology for different reasons, such as economic, ethical and religion (Apampa et al., 2008).

3.7 Continuous and Transparent Authentication

During the last decade, an interesting, less effortful and new class of security mechanism has been proposed and referred to as continuous authentication, the identity of an individual is frequently verified for the entire period of the session (Clarke, 2011; Traoré & Ahmed, 2012), to offer a technique that runs in the background without requiring explicit user interaction (Crawford & Renaud, 2014).

The principle of continuous and transparent authentication represents an essential mechanism in this project, in which the study needs it to ensure a full monitoring for the online assessment which should be transparent enough to provide the candidate with an acceptable level of satisfaction during taking the exam, as the examinee should not be bothered or interrupted due to the importance of the exam. Therefore, for continuous biometric authentication, the more transparent (user-friendly) modalities employed the more convenience the examinee experienced. Some studies which have been discussed in the previous chapter have proposed continuous and/or to some extent transparent authentication. However, other studies regarding this concept can be mentioned here.

Having conducted the literature review process, over 30 studies have been identified into multimodal biometrics; however, the selection has been done in order to provide a comparison of different modalities across different types of studies (e.g. PC, mobile, and wearable devices). As a result, a dozen of studies has been summarised in Table 3.3 below. The commentary that follows describes each one in more detail.

	Author(s)	Context	Biometric Modalities	Performance (%)	Other Features	Participants	Duration	Type
1	Clarke and Furnell (2006)	Mobile	Several biometrics	FAR 0.00002 FRR 0.4	Intrusive login using a secret code	-	-	Conceptual
2	Sim et al. (2007)	PC	Fingerprint & Face (extendable)	-	Holistic fusion New performance metrics	11	30 min	Real
3	Ojala et al. (2008)	Wearable & Laptop	Fingerprint & Soft biometrics	Matching 40-60	Additional wristband Intrusive login using fingerprint	-	-	Prototype
4	Clarke et al. (2009)	Mobile	Face, Keystroke & Voice (extendable)	EER 0.01	Standalone & client-server modes	27	45 min	Real
5	Niinuma et al. (2010)	Laptop	Face & Soft biometrics	FAR 0 FRR 4.17	Intrusive login using a secret code	20	-	Real
6	Soltane et al. (2010)	PC	Face	EER 0.449	Adaptive Bayesian fusion method	30	3 sessions	Simulation
			Voice	EER 0.003				
			Overall	EER 0.087				
7	Li et al. (2011)	Mobile	Telephony	EER 5.4	-	76	-	Simulation Offline dataset
			Texting	EER 2.2				
			Apps services	EER 13.5				
			Overall	EER 7.03				
8	Crawford et al. (2013); Crawford and Renaud (2014)	Mobile	Keystroke	EER 10	67% reduction of explicit authentication	30	7 tasks	Real & Simulation
			Voice	EER 25				
9	Saevanee et al. (2014)	Mobile	Behavioural profiling	EER 9.2	91% reduction of explicit authentication	30	-	Simulation Offline dataset & Real
			Linguistic profiling	EER 12.8				
			Keystroke	EER 20.8				
			Overall	EER 3.3				
10	Ceccarelli et al. (2014)	Web	Voice	FMR 10	Intrusive login using fingerprint	-	-	Prototype
			Face	FMR 2.58				
11	Tsai et al. (2014); Khan et al. (2011)	Laptop	Face & Soft biometrics	Recognition 86.88	Swarm intelligence algorithms	7	-	Real

Table 3.3: Continuous and Transparent Multibiometric Authentication Systems

The Intelligent Authentication Management System (IAMS) is a mobile-based system that has been proposed by Clarke and Furnell, (2006), in order to offer transparent and continuous authentication, they combined secret knowledge-based method and available biometric techniques. Both standalone and client-server modes have been proposed to operate this system. While the approach achieved the required performance with FAR of 0.00002% and

FRR of 0.4%, the method inherited the defects of the secret knowledge-based approach in spite of its simple use at the initial entry.

Moreover, Clarke et al., (2009) extended the aforementioned IAMS by the implementation of Transparent Authentication Systems; they conducted further mobile-based solution employing Non-Intrusive and Continuous Authentication (NICA). It uses a combination of secret knowledge authentication with several selected biometric methods. It is able to choose particular biometric modalities to authenticate a mobile user relying on the configuration of their device. Thereby, in case the camera is damaged, the system would select speaker recognition and keystroke analysis to be employed for user authentication. To evaluate the approach, 27 participants were tasked for 45 minutes. EER of less than 0.01% were recorded. Nevertheless, in order to alleviate the error rates of the deployed biometric algorithms, they reduced the threshold, consequently, this would impact the accuracy of this result.

Another empirical mobile-based solution has been conducted by Soltane et al., (2010) involving 30 participants for 3 separate sessions, the method uses face and voice verification during the experiment. As a result, it accomplished a performance for both face and speaker recognition of 0.449% and 0.003% EERs respectively. Although the results might be affected by the individual fusion technique, the overall EER was 0.087% when utilising Adaptive Bayesian fusion approach. Albeit this result is better than the EER of previous facial recognition, it is yet worse than the voice's. However, there is still an essential need for involving multibiometric mechanism in order to harden the system against any potential attacks.

Crawford and Renaud (2014) and Crawford et al (2013) suggested readily available behavioural biometrics (voice recognition and keystroke dynamics) to acquire a level of transparent and continuous authentication. Both studies are proposing secure framework for smartphone and reporting encouraging experimental results. Crawford and Renaud found that 90% of 30 surveyed persons, which completed a series of tasks on a smartphone, agree with the idea of using transparent authentication on their mobile device. The second study showed that there is a significant improvement in the usability of the mobile thereby utilising transparent authentication method. However, the experiments do not take in account the limitations of every mobile device. Furthermore, these two studies/results are restricted and implemented on merely smartphones environments and ignored the wide range of other

devices that the user would utilise including but not limited to personal computers and tablets.

In one of the newest field of studies, Ojala et al., (2008) attempted to build a prototype of a wearable continuous and transparent authentication for wristband device. The fingerprint recognition has been used for individual verification (at the login stage), yet the user continuous authentication has been achieved by measuring the skin temperature, heart rate and the body capacitance. Although it is new and interesting approach, weakness, however, can be addressed such as: the intrusiveness of login process because of providing fingerprints information, and the matching scores were low (from 40 to 60%).

To balance between the usability and security of the Internet service and consequent client satisfaction, an effort to exploit the advantageous features of transparent authentication technique was proposed by Ceccarelli et al., (2014). They offered a multimodal biometrics Federated Authentication using the Cloud authentication protocol applied in an Internet system named Context Aware Security by Hierarchical Multilevel Architecture (CASHIMA). It is supposed to operate securely in any web service from a variety of client devices, employing accessible biometric sensors of fingerprint, voice, face, and/or keystroke dynamics samples. It implements a changing level of trust in the individual similar to the idea of transparent authentication system confidence, in that it is determined according to the intervals and quality of the collected samples. The authentication level reflects on the subsequent services the individual is allowed access to and the risk level linked to them, causing related reaction ranging from granting access to sensitive services, limiting access to some services, to locking out the system and requesting re-verification. However, in terms of usability, the same sessions have been used extensively by the client device which leads to emergence a problem of battery consumption. Furthermore, although they developed and exercised a prototype, there is no complete assessment of the solution to verify the feasibility of the approach. Finally, this approach would suffer from a problem of the growing profile of the client, because of there is too much of the acquired biometric data which depends on the client's usage of the device.

The passive usage of several biometrics utilising a protected computer encourages Sim et al. (2007) to propose a multimodal biometric verification system that continuously authenticates the presence of a logged-in user. They experimented with the deployment of facial and fingerprint recognition characteristics. To secure the system, a set of security policies has

been enforced, responding to the user authentication fails, by stopping the computer or user's processes that are executing in the operating system. The authors claim that their implementation in such system was the first. Nevertheless, neither enough number of users nor sufficient period of time has been conducted to prove the system usability test in this study.

Further approaches were suggested combining facial recognition as a strong physiological biometric modality along with soft biometrics such as face skin colour and clothes colour, aiming at offering continuous authentication that can be accomplished passively. Khan et al., (2011) and Tsai et al., (2014) achieved the same work that followed this approach, so they are referred to here as one, both were tested on laptops, in which the authentication process starts intrusively via the login employing either password or face recognition, then continually matching the soft biometrics histogram against what was collected at the login stage. This study has scored recognition of 86.88% of only 7 participants utilising swarm intelligent algorithms. In a similar study, Niinuma et al., (2010) also proposed blending the face recognition with soft biometrics, they accomplished 0.0% FAR and 4.17% FRR in an experiment involving 20 participants. Aside from the relatively small number of participants in these studies that would not reflect the real implementation, the intrusiveness of the potential repeated authentication because of the variation of lighting throughout the usage session causing user inconvenience.

More research in the similar context depends on behavioural biometrics has been proposed by (Li et al., 2011; Saevanee et al., 2014). The first research achieved the dynamic user profile of the usage of calling, text messaging, and general applications services on mobile phone with an EER of 5.4%, 2.2% and 13.5% respectively and an overall of 7.03%. The second employed linguistic profiling, keystroke dynamics and behaviour profiling with an EER of 12.8%, 20.8% and 9.2% respectively and an overall of 3.3%. They argued that these methods would diminish the intrusive authentication requests of traditional methods by 91%. However, they did not reflect the real usage of an individual, as they were completely or partially acquired based upon desperate and limited offline datasets. Moreover, the number of subjects is limited and the employed dataset is old (dated back to 2004) when the abilities of the cell phones were limited.

It is clear that the success of a specific transparent and continuous authentication approach can provide both effective security and user acceptance. However, it is essential to have a

high level of performance, scalability, and interoperability among and with existing and future systems. Moreover, all these requirements should be implemented and evaluated comprehensively on real data in order to prove that such a method is feasible and should be put and deployed in an operational context to measure other aspects that are essential for successful adoption (e.g. acceptability and usability).

3.8 Biometric Transparency, Applicability, and Satisfaction in E-Assessments

Generally, researchers have relied on one or two biometric features of the candidate during the exam. Table 3.4 summarises the transparency, user satisfactory, and applicability of the human biometric features which have been proposed by different researchers or applied by many commercial companies until the moment, as well as to some modalities that could be employed in future.

✓ = Yes; X = No; ? = Not sure because it has not been applied in such system till now.

Biometric type	Transparency	User satisfaction	Applicability in e-assessments	Used/Proposed
Face	✓	✓	✓	✓
Iris	possible	possible	✓	✓
Keystroke	✓	✓	✓	✓
Mouse	✓	✓	✓	✓
Speaker	✓	✓	✓	✓
Fingerprints	X	X	✓	✓
Handwriting	✓	possible	✓	✓
Eye movements	✓	?	✓	X
Head movements	✓	?	✓	X
Linguistic	✓	?	✓	X
Facial thermogram	✓	?	possible	X
Keyboard sounds	✓	?	possible	X
Eye blinking	✓	?	possible	X
Lip motion	✓	?	possible	X
Behavioural profiling	✓	?	possible	X
Ear geometry	✓	?	possible	X
Palm print	possible	?	possible	X
Acoustic ear	possible	?	possible	X
Vascular pattern	possible	?	possible	X

Table 3.4: A Comparison of the Human Biometric Features in E-Assessments

Face recognition, as a user-friendly mechanism of candidate authentication, is the main authentication approach that has already been suggested and used in the primary prototype e-

invigilation system (as described in the Chapter 5). Beyond face, many of the other proposed biometric modalities require further research. For example, although many practical studies argue that the required time for data collection of mouse dynamics is very long to complete, the ease of use, popularity, and the high level of transparency of the mouse interface (e.g. for multi-choice) encourages combining it with other more robust biometric techniques (as secondary and soft biometrics to empower the authentication level). The low-cost and effectiveness of keystroke recognition (e.g. for essay writing), in addition to the wide use of keyboard interface in the e-assessment environment, are also encouraging. However, both of these techniques require further research to explore how enrolment can be undertaken in a usable and effective manner and to ensure the biometric performance achieved is sufficient. The same can be said for utilising linguistic analysis (e.g. essay writing) or speaker recognition (e.g. oral questions).

Iris recognition offers an interesting opportunity as it is generally considered to be a highly reliable modality with robust performance. However, current implementations require a sensitive near-infrared camera. Web cameras, to date, have not been utilised as a sensing technology. In either case, obtaining a complete iris image is also a challenge, as the eyelid will frequently obscure the eye. Research has not thoroughly investigated to what extent a partial iris image is useful in providing identity verification and to what degree of performance.

Furthermore, employing soft but robust, feasible and flexible biometric authentication (i.e. eye and head movements which are the newest field of research), as additional non-intrusive modalities could improve the performance of the invigilation processes in e-assessments dramatically. Although both have been suggested as secondary biometric modalities, research proved a high level of accuracy achieved. This opens the door for using them as primary transparent and continuous authentication methods.

There is no doubt that utilising and merging the above discussed biometric techniques can effectively help to detect/prevent the potential threat of cheating, fraud or spoofing by the exam's taker or any unauthorised help by anyone in their surrounding environment during the online exam time. In general, the feasibility of using the above biometric techniques for securing e-assessment environments can be summarised as:

1- Cost; each technique is relatively inexpensive because the devices that will be utilised in the system are commonly attached to computers (or can be considered likely to be more common in the future).
2- From a practicality and applicability perspective, five of the nine proposed techniques have been proven to be used effectively for electronic surveillance purposes, and have been utilised for the purposes of monitoring in online exams environments in previous studies.
3- From a user-friendly (non-intrusiveness) viewpoint, each of the proposed techniques depends on devices for biometric sample acquisition which have a high level of transparency that gives the ability to complete the process without inconvenience (potentially without the knowledge of the candidate).
4- From a continuous monitoring perspective, each of the suggested techniques can achieve this principle efficiently and effectively.
5- From the user privacy point of view, most of these technologies (especially the behaviour biometrics ones) should not have any untoward side effects.
6- Due to its transparency and reliability, Intel RealSense facial recognition has been chosen to be the main authentication approach in the proposed architecture of the e-invigilation system.

3.9 Conclusion

Given the three authentication approaches: something the user knows (such as passwords), something the user has (such as SIMs) and something the user is (biometrics), biometric techniques outperform the other two methods by identifying a person based upon their unique characteristics. It is the only possible method that results in improving the level of security provided in a convenient fashion. It has been identified that authentication of the individuals can occur transparently enabling them to be authenticated numerous times without any or with minimal inconvenience (or even passively), as samples are collected during an individual's normal interaction with the device. While the physiological methods offer solid protection as they are highly unique and very difficult to forge, the behavioural methods on the other hand tend to provide more transparent authentication. However, with the ongoing development of biometric technologies and algorithms, facial recognition currently could continuously achieve both robust and transparent authentication principles.

Generally, the main weakness surrounding biometrics is the accuracy of the methods, with approaches varying in strength from very strong methods (e.g. retina recognition) to weak techniques (e.g. behavioural profiling). Nevertheless, no matter how robust a method is, the effectiveness of differentiating between individuals is determined by the threshold level. A poorly selected threshold level in retina recognition could degrade its performance below a well selected threshold level in behavioural profiling. Thus, it is vital to select the threshold levels properly for specific techniques and perhaps even on a per individual basis.

In prior studies, the range of the utilised/proposed modalities are rather limited, some of them are rather behavioural based which is likely to lead to high level of error rate. Using a multimodal continuous system might provide more reliable samples and offer higher performance. The nature of the transparent and continuous biometric domain (as illustrated in Table 3.3) has shown a good range of studies have been done currently within a range of different contexts and can lead into a good level of performance, therefore, considering it useful in e-invigilation might not be a bad idea.

Among the physiological biometric modalities, the face can be considered the most transparent with a high potential of user satisfaction, and applicable to be used effectively to support e-assessment security. Whereas iris could be applied for authentication in e-assessment (Bal and Acharya, 2011), it still needs to be secondary rather than the main biometric modalities. On the other hand, keystroke analysis, mouse dynamic, and speaker recognition behavioural biometric modalities are of the most transparent and applicable in e-assessments achieving good user satisfaction. However, most of the studies have presented satisfactory performances feasible for verification mode of these behavioural biometrics or for identification only and only if combined with other authentication methods. Therefore, they are also still secondary more than the main biometric modalities. Moreover, from the analysis across this chapter, eye and head movements can provide promising alternatives.

4 EIEA Architecture

4.1 Introduction

Due to the essential need for a robust, convenient and universal authentication scheme that can be achieved flawlessly in a location, technology and service independent manner, in this chapter, the focus has been on the development of a more secure invigilation for e-assessments, capable of exceeding the related limitations imposed by invigilated e-examinations, in order to provide a flexible, transparent and continuous identity verification and security method.

The following sections present a theoretical model of E-Invigilation of E-Assessment (EIEA) system architecture proposal including a detailed discussion of the architecture requirements, components and complete design to be the core of the system which captures, processes, and monitors students in a controlled and convenient fashion, and a detailed description of the system processes and procedures that enable such flexibility are presented.

4.2 System Requirements

As demonstrated in the prior art, the idea of developing a system that takes the role of the physical proctor (human) can face lots of challenges, barriers and requirements in order to reach an acceptable level that enables this system to be suitable.

From the literature in Chapters 2 and 3, the following requirements were derived:

- The system should have the ability to continuously monitor a user by biometrics means in the most convenient fashion.
- The system should be secure against external and internal threats.
- The system needs to use effective mechanisms to mitigate cheating.
- The system needs to be scalable to manage the storage, retrieval and processing of biometric samples.
- A system that is flexible to enable it to adapt to new monitoring and biometric technologies.
- The system should provide academics with a prioritised and usable interface to verify and check cases of possible cheating.

- A system that is user-centric (through the application of HCI principles).
- The system should be platform independent.
- The system needs to minimise specialist hardware.

It is important that the system is not restricted to current technologies (both sensing technologies and biometric backend systems) so that it can adapt to new modalities and new classification algorithms. Providing a user-centric approach to the design should make this achievable by providing administrators with the ability to add and remove security modules to/from the system. The user-centric design has also helped ensure both assessors and participants are provided with a system that is naturally intuitive and requires minimal learning.

Whilst the biometric-based approaches provide a basis for continuously verifying the authenticity of the participant, the system also should be hardened against attack – from both internal and external threats. It is essential that no component of the system is vulnerable. Given the nature of the data being held (i.e. biometric-based), it is also important the system maintains the security and privacy of participant data.

By utilising a range of efficient biometric approaches, the proposed e-invigilation system can easily adapt to differing inputs (e.g. keyboard or mouse) depending on the nature of the exam questions set. Through this approach, a single assessment will provide the assessor with a range of biometric samples from which the system can verify and subsequently flag any potential misuse. A key difference in the approach taken in this research is that the biometrics are not used to provide or deny access but merely as a tool for the assessor to be able easily to identify and investigate participants.

A further requirement that was deemed essential in this research was the need to remove any financial burden upon the participant. In order for e-invigilation to be widely adopted and successful, it is imperative that it should not rely upon specialist hardware or sensing devices (such as the Securexam Remote Proctor System – section 2.2.4). Participants could not be expected to have to purchase specialist equipment in order to take an examination nor attend a specialist testing facility. Fortunately, modern computers have a range of biometric sensing technologies as standard – web camera, keyboard, mouse, touch screen, or microphone that could be used in this context.

All these system requirements have been met by utilising the combination of processes within a novel multimodal biometric framework. The framework employs a combination of system-level monitoring and multiple transparent authentication techniques (Non-intrusive techniques are used to ensure student's legitimacy). The result is an advanced authentication system that can provide transparent and continuous identity verification to the exam taker with minimum inconvenience.

4.3 The Architecture

From students perspective, there is no doubt that one of the most important principles is the maintenance of a convenient testing mechanism, however, from academics point of view, the primary concern is maintaining a secure, controlled test environment to minimise academic dishonesty. Whilst research has begun to propose solutions to enable the student to take assessments remotely, they fundamentally fail to provide the integrity required (as discussed in Chapter 2), therefore, the following proposed architecture can be considered as an intensive development of a robust online monitoring environment that can provide the same or better levels of security than current physical centres provide. The presentation will include the development of novel continuous identity verification approaches that will underpin the e-invigilation framework. A thorough systems-based analysis will also be undertaken to mitigate the threat assessment.

To increase the level of security, various monitoring approaches have been incorporated, including continuous eye tracking, operating system monitoring, and network monitoring. However, in addition to the means of detecting cheating and misuse, the system also tries preventing cheating as well, for example, banning test takers from reaching computer resources, taking the exam at a later date other than the one determined by the responsible academic, or surfing the Internet.

This novel e-invigilation system is designed in a modular fashion to incorporate a range of behavioural and physiological biometrics (the most user-friendly and robust techniques). This range of techniques provides an opportunity to capture biometric samples under a range of differing examination scenarios (e.g. essay writing, multiple choice test). The key to user acceptance is usability and the system has been designed to specifically ensure ease of use for all users. The overall architecture of the proposed E-Invigilation of E-Assessments (EIEA) system is depicted in the following Figure 4.1.

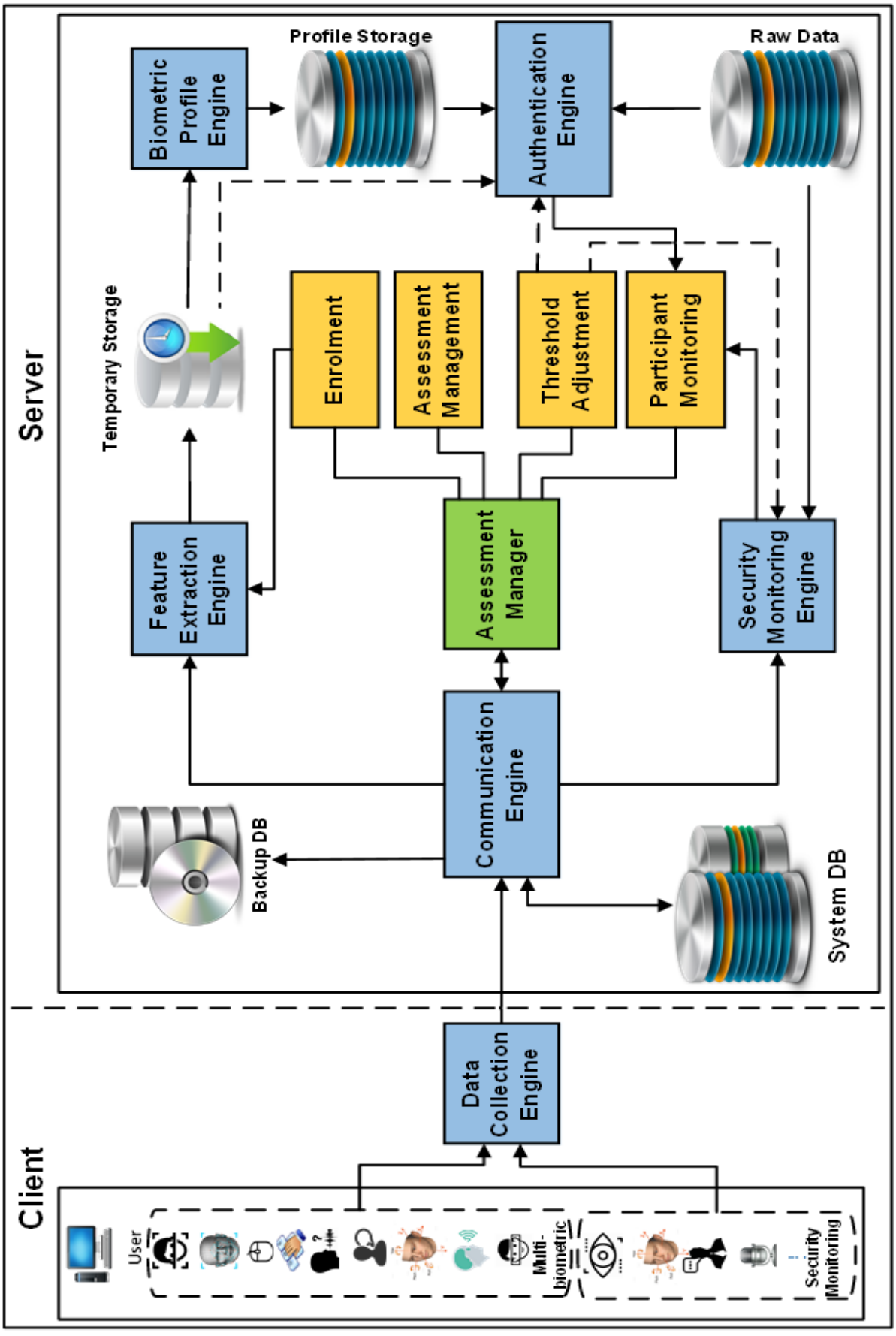


Figure 4.1: Overall EIEA System Architecture

The architecture has been designed around two operational objectives: continuous biometric-based monitoring of the participant and system-level monitoring to prevent cheating. On top of this, there is a variety of management-level functionality that provides the basis for creating and managing assessments. This can be identified within the architectural diagram as the *Data Collection Engine, Feature Extraction Engine, Biometric Profile Engine, Authentication Engine, Security Monitoring Engine, Communication Engine,* and *Assessment Manager* respectively. All communications between the client and e-invigilation system have been secured (using Transport Layer Security (TLS)). In order to aid the interoperability of biometric samples, biometric sub-systems (feature extraction and classification), the architecture is developed with the relevant ISO standards (ISO 19794, ISO 19785 and ISO 19784) in mind (ISO, 2006a, 2006b, 2011).

When it comes to the implementation, the above client-server architecture is a platform independent design in which can be implemented via browser as it is a largely web based driven, and this makes it a lot easier in terms of usability. Currently, some security aspect of the architecture cannot be supported just from the browser; therefore a small agent or application will be needed on the system itself to do a degree of monitoring. It is envisaged that the control of the sensors (e.g. eye tracking security) would be possible via the web browser (as the microphone and camera are today). This will allow for a more interoperable and cross-platform solution. However, in the near-term, the architecture has also been designed with a client-side agent-based approach that provides that level of interaction and interoperability.

Moreover, the system enables the student to use any available device connected to the Internet to undertake the e-assessment, for example, he/she has the ability to just pick up his/her tablet, smartphone or a laptop, with any operating system such as Mac or Windows, and log in and then the model should work efficiently. In the case of mobile platform, there is a need for a small app that from screen perspective just puts the user on the browser, but it also provides the ability of monitoring and capturing the required information. Both the small agent and mobile app would be accessible and downloadable via the e-invigilation website. An example of how the system would work in reality is shown in Figure 4.2; this presents an illustration of how the interaction could be accomplished between the client and the server.

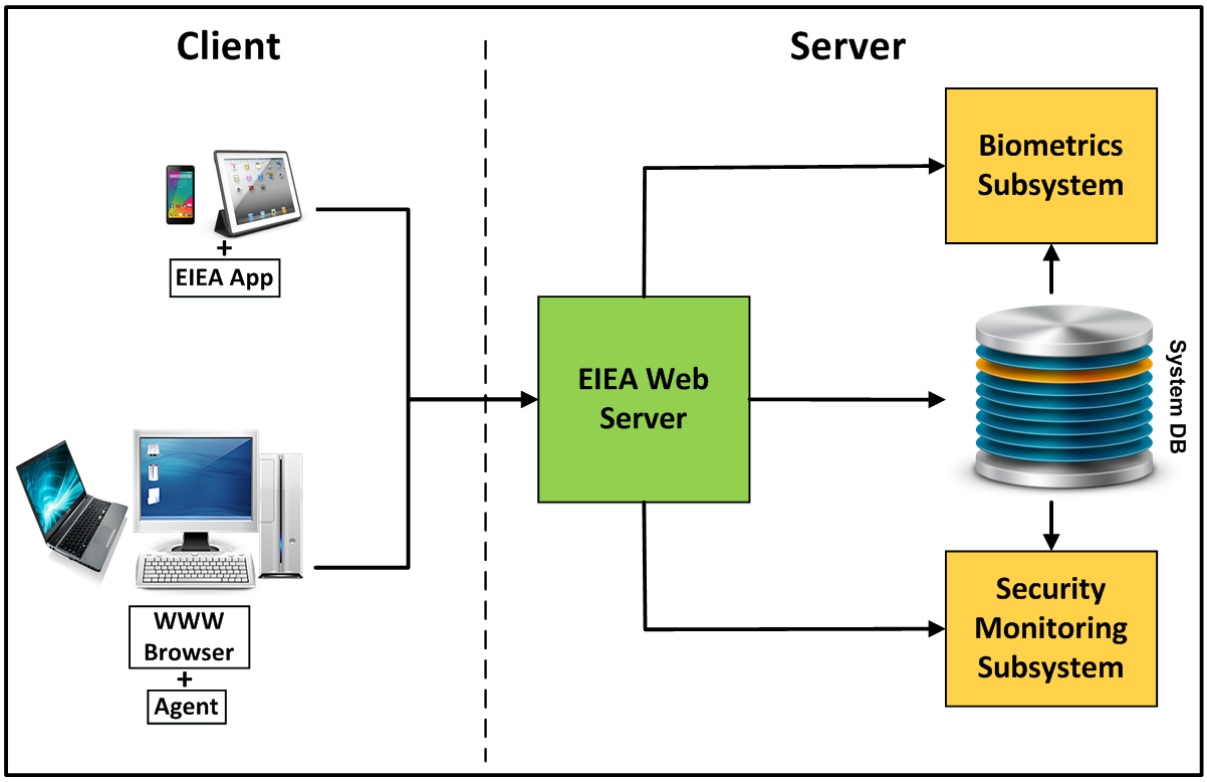


Figure 4.2: The Interaction between the Client and the Server in the System

The users of the system will communicate with a central web server that handles most of the system processes, for instance, it contains each of the data collection engine, communication engine and assessment manager, these functionalities in turn communicate with the rest of system components including the biometric subsystem for continuous identity verification, system database for storing/fetching or backup/recovery data, and security monitoring subsystem for detecting misuse and preventing or minimising the opportunity for cheating.

4.3.1 System Database Design

In order to achieve a complete theoretical design, a database for undergraduate teaching in the university will be utilised, the basic attributes to build the required database as efficient and brief as possible are needed to be defined. There are two points of view that have been put in the designer mind when designing such system: academic point of view and student point of view, in which both of them are the end users of that system.

The following Entity Relationship Diagram (ERD) shows the high level system database (Figure 4.3) which has been designed to be the base for the practical database design in the next Chapter 5.

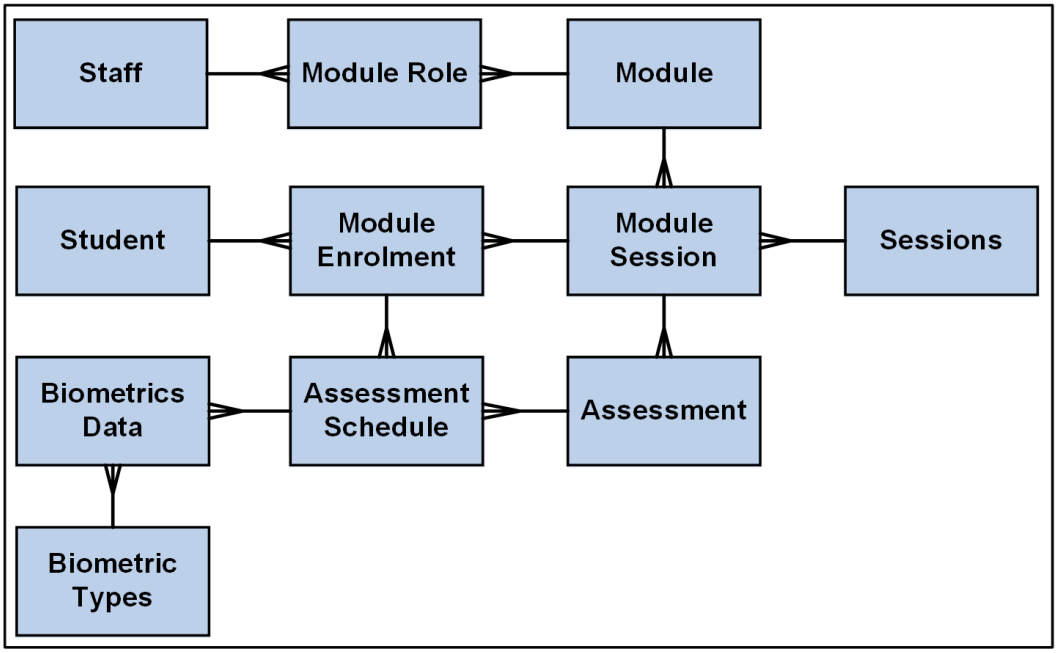


Figure 4.3: EIEA ERD Diagram

The Database consists of the following tables:

- Staff, includes the details about the academic.
- Module, contains all Modules.
- Module Role, a joint table between Staff and Module.
- Student, includes the details about the student.
- Module Session, a joint table between Modules and Sessions.
- Module Enrolment, a joint table between Student and Module Session.
- Sessions, for every module there are many sessions.
- Biometrics Data, contains the raw biometric data.
- Assessment, contains all the details about the created assessment.
- Assessment Schedule, a joint table between Module Enrolment and Assessment
- Biometric Types, connected to the Biometrics Data to indicating the type of particular biometrics available currently and providing the ability to add/remove biometric modalities according to the system need.

4.3.2 Architecture Components and Processes

The proposed system is not an e-assessment system – there are already very comprehensive systems in place that do this – but rather an over-arching system that provides the monitoring and tracking of participants during an e-assessment. It is also important to ensure the system has a wide compatibility and is not tied to specific hardware, software or operating systems. The architecture itself is fundamentally set around three primary roles: the admin that gets to define set of characteristics and the underlying operations such as which modalities can be universally used across the platform; the academic that has ability for setting up a new

assessment, checking assessment and reporting; and the student who enrols and uses the system.

4.3.2.1 Robust and Transparent Multi-Biometric Monitoring

As concluded in the previous chapters, it is necessary to rely upon more than one biometric trait to implement the idea of providing a secure online assessment given the range of assessment types and hardware availability. Therefore, this research proposes the use of multi-biometrics as a robust, reliable, secure and convenient process of continuous non-intrusive verification beyond the initial identification or login process. Even though transparent multi-biometric authentication is a developing technology and it has not been suggested widely in many studies with respect to e-assessment, however, this research seeks to combine many biometric techniques including but not limited to: 2D and 3D facial recognition, mouse dynamics, keystroke analysis, voice verification, linguistic analysis, eye movements, head movements and iris recognition in order to achieve and guarantee a secure online assessment environment.

The system is flexible that enables the administrator to easily add or remove variety of authentication mechanisms, the biometrics can be simply added or removed to/from the biometrics list in the system database, the system then automatically adapts to the new situation. The level of authentication depends on the exam nature (e.g. multiple choice or long answer questions), the devices/sensors that available during the examination, and the level of security that the academic would like to achieve. For example, if a system utilises a set of robust physiological biometric modalities, and a decision has been made to use/append mouse movement as a behavioural biometric modality during particular assessment to add a further layer of transparent biometrics in order to improve the authentication (it would be done mostly by the examiners or the examination institution – however, these sorts of decisions also would be taken after a recommendation provided by a system developer/administrator depending on variety of factors, for instance the level of security achieved or the feasibility of utilising a particular technique), the academic then simply selects this required biometric modality among a range of available (extendable) list of modalities in the Assessment Manger (as depicted in Figure 4.4). The system then adapts everything automatically to involve the new authentication mechanism, starting from the data collection process to the reporting of misuse procedures. The administrator (or a recommendation by the administrator to the academic) is also responsible for deciding the

number of samples of each modality would be captured during the data collection stage, for example, for face recognition a sample of the user face would be taken per -/+3 second. Furthermore, the academic could decide only allow the participants to take a test if a particular predefined list of biometric modalities is available (for instance a list consists of 2D Facial Recognition, Voce Verification and Keystroke Analysis), otherwise, they cannot take that test, which means they have to get the mandatory technology firstly. A check – to discover whether the utilised machine has these devices or not – could be done by a web browser (e.g. Google Chrome) or by the client, for example, looking for the microphone and the camera to take the control over them. Therefore, if the machine does not have the required sensors/devices/technologies then the system will not allow the student to take the e-assessment (for instance, if it is not able to sense a 3D camera, then it will come up with a message saying "Unfortunately, you need to use some other technology that has this camera").

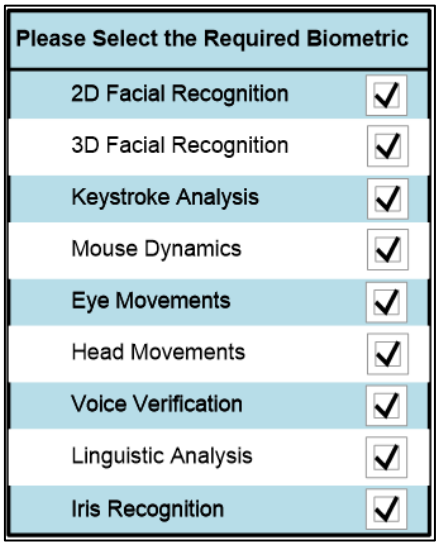


Figure 4.4: Example of How to Add/Remove Biometric Modality

Therefore, using this list will simplify the process to the academic to add/remove modalities that are enabled by the system (as they are compatible with the system). Furthermore, the system is also not restricted to current technologies (both sensing technologies and biometric backend systems) so that it can adapt to new modalities and new classification algorithms. The main idea here is the system will be continuously capturing different biometric modalities. Therefore, the architecture is built in a modular fashion that accepts any form of biometric modality as long as it is ISO compliant, and it will store, capture and process this information. For example, if a decision has been taken to add new strong modality which has not been defined basically in the system, then the admin of the system needs to have a

functionality where he/she can add new biometric, thus the system will open a wizard that allows the admin to give it a name which then allows the database to be updated to know that the new modality exist. But it needs additional code built into the Data Collection Engine to know how to capture and process it. Therefore, on the current version with an agent, it will require an agent update (the update will be done to the code that required to do that capturing). On the other hand, with a browser-based version (assuming the browser supports particular capture device), it is just the browser code needed to be updated. For example, if the new modality needs a web camera then it is probably already enabled to do facial recognition, but the capture will be coded.

As one of the main system architecture requirements is to design an authentication mechanism that will automatically work on all devices that enables the framework to plug-in to the different operating systems (the framework is system- and device-independent), therefore, a wide range of devices can be used for achieving the e-assessment (e.g. laptop, desktop, tablets or smartphones), which vary in terms of their hardware configurations and operating systems. Most current biometric data collection device manufacturers ensure that these devices support variety of Operating Systems such as Windows, Mac, Android, or Windows Phone, thus the system is developed as Universal application. The system includes a Compatibility Table (as illustrated in Table 4.1 – populated as biometric samples are collected and templates created) that presents an extendable list of compatible authentication techniques for different devices.

ID	Technique	Device Compatibility	Template Gen Date
1	Face	True	18/11/2016
2	Voice	False	-
3	Finger	-	-
4	Mouse	True	12/11/2016
5	Keystroke	True	22/10/2016
6	Iris	False	-
7	Signature	-	-
8	Linguistic	True	10/11/2016
9	Eye	True	25/10/2016
10	Head	True	-
11	3D Face	False	-
..	……..	…….	……..

Table 4.1: Compatibility Table

The *Technique* column of the table defines all the BioAPI compatible devices. The *Device Compatibility* column enables the system administrator to disable any of the techniques that are enabled by the Hardware Compatibility – this might be desirable for a user who has difficulty in using a specific authentication method, an academic would like to change the level of security, or for any network relevant reasons. The *Template Gen Date* column shows whether a valid template has been generated. Because it is the administrator's job to link in to the recognition systems that operate in the background, therefore he/she should define which biometrics initially could be included in the system. Therefore, an academic cannot select biometric modality from which an administrator has not enabled, but an academic could select the subset and equally a user could select the subset of the academic, and that provides flexibility according to the nature of the examination process, the hardware that available, or even the applicability to be implemented by the student.

To ensure providing all the hardware dependent information to the framework, the following Table 4.2 is also required (Algorithm Location table). Therefore, this table, upon system installation will be empty and it will need the administrator to go in and define which biometric modalities exist and where they are stored.

ID	Server DLL Location
1	\\server\Iibra\face.dII
2	\\server\Iibra\voice.dII
3	\\server\Iibra\mouse.dII
4	\\server\Iibra\keystroke.dII
5	\\server\Iibra\iris.dII
6	\\server\Iibra\linguistic.dII
7	\\server\Iibra\eye.dII
8	\\server\Iibra\head.dII
.	……

Table 4.2: Algorithm Location Table

The *ID* value within the *Compatibility* table corresponds to the *ID* value in the above *Algorithm Location* table, which details the file physical location of each of the authentication techniques library file. It is these library files which hold the procedures for template generation and authentication.

4.3.2.2 Data Collection Engine

The primary role of the Data Collection Engine is to capture a user's input interaction. Although the platform independent that the system supports, the actual samples to be captured by this engine will be dependent upon the hardware contained within or connected to the machine being used for taking the online assessment. However, the system allows the users to decide the level of security during the selection of biometric modalities or the security mechanisms to be involved. This system is designed and developed to work with samples that can be captured transparently as identified in Chapter 3. The Data Collection Engine, as shown in Figure 4.5, contains a number of interfaces that will be utilised in order to capture the input data, each of these interfaces captures and logs samples from their respective input devices (Currently it could be either the agent or the Data Collection Engine – depending upon whether the web browser supports the functionality or not).

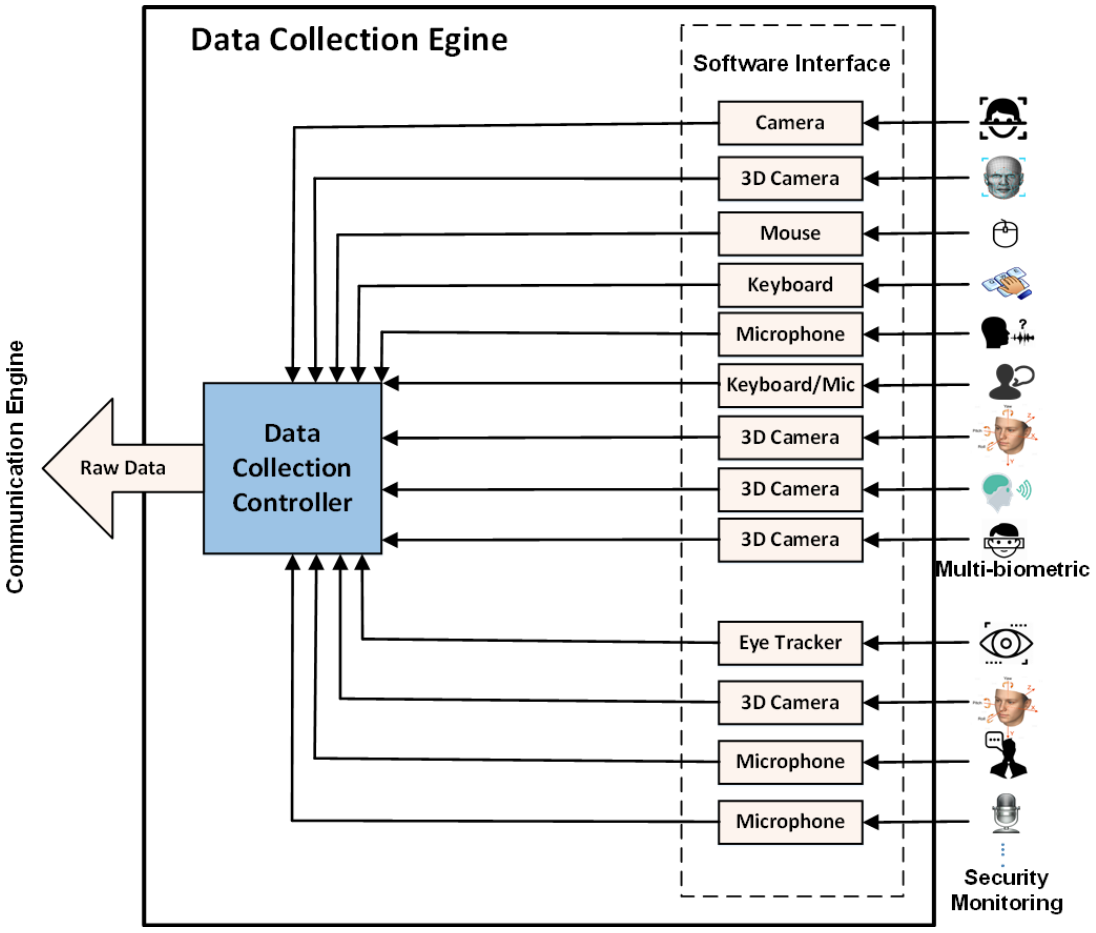


Figure 4.5: Data Collection Engine

To provide continuous identity verification, Data Collection Engine would basically be able to collect samples from different biometric modalities (multi-biometric model). Furthermore,

in order to maintain security several mechanisms have been developed to enable continuous monitoring of the system, these include for instance the use of microphone to record and store the entire section, and the use of that recording to be pre-processed to provide voice recognition, or to understand what has been talking about (e.g. does it words, question being asked, unauthorised help, or information about the assessment coming up in that audio stream). It is also possible to collect student's eye movements from the 3D Camera or Eye Tracker device whilst the student is reading/interacting with the machine during the exam (for detecting the eye positions whether it is within the screen boundaries or not. With the same former sensors, student's head movements from the 3D Camera whilst the student is interacting with the machine during the exam (for detecting the head positions whether it is within the predefined angles that specify whether he/she was looking at the screen or not).

There would be potentially some hurdles to overcome in terms of how to build the browser compatibility with certain biometric sensors (that is why the agent was included in the architecture design), however modern web browsers today already support functionality of capturing the camera and microphone, therefore, it is not a huge stretch in the imagination to believe that future version of modification would exist that the browser can be developed in order to capture functionality of other hardware based devices also (e.g. 3D camera with infrared sensors).

When the online assessment has finished, the Data Collection Controller will send all this processed and analysed data (along with all the relevant activities that the security algorithms were collecting during the misuse detecting processes) to the Communication Engine which keeps them into the System Database against a particular record of the student ID that have taken this test. Therefore, the relevant data will not be stored directly in the System Database as the system will not enable a direct feeding of this data to the database without some form of checking whether the data is valid in the first place, and this checking process will be implemented in the Communication Engine. The data will finally be stored in the following Student Biometric Data Table 4.3 (Physical Location field).

Student ID	Biometric ID	Physical Location
1	1	\\server\students\1\1
1	2	\\server\students\1\2
1	3	\\server\students\1\3
.	.	……

Table 4.3: Student Biometric Data

Then once this stage is completed for all the e-assessments, the system (Communication Engine) will send an email, to the relevant academic that created this assessment, tells that the data collection and processing have finished and the data is ready to be reviewed, the academic could then log in the system and send a command to the system (via the Assessment Manager as described in section 4.3.2.8) in order to establish the individual reviewing to take the final decision (deny or confirm cheating).

In terms of data sizes on the disk, the most substantial data would be the facial images and sound files. For instance, in Chapter 6, the experiment results show and support this fact, in which 306 MB is required for all face images and 612 MB for all audio recordings (both are 918 of 978.1 MB of the total data size of all participants). Particularly, these two data types are required to be stored in order to achieve the proposed participant monitoring both for authentication and security purposes. However, the system also stores the rest biometrics and security information (e.g. mouse movements, keystroke analysis, head movements, eye movements) as they are light and will not be considered as heavy volume of data to be stored – might be temporarily for later processing. For example, in the same aforementioned experiment, the space of only 30.6 and 25.5 MB is required for both eye and head movements respectively for all participants through the entire experiment. Generally, given the volume of the information that the system could capture from a number of e-assessments involving a large number of students, it would be desirable to minimise this volume of the collected information. Therefore, the academic/institution could, for instance, reduce the volume of data by increasing the capturing time (e.g. captures the sample every X + Y seconds which is dynamic rather than the static predefined/default X seconds, where X and Y > 0). The quality of the collected samples and the recorded sound could also be reduced in order to save far less volume of data on the disk. Furthermore, according to a policy that can be decided by the institution conducting the e-assessment, the academic could have the ability to destroy the raw data whenever there is no need to keep them, for instance, if the academic completed the monitoring through the Assessment Manager (i.e. Confirms or denies cheating), and after a period of relatively long time (e.g. after one year as the student moved to another stage or even after many years when the student has graduated), as the academic feels there is no need for keeping the raw data, then he/she can only keep a light version of these data (metadata) alternatively – so the process is not about the deletion of data in the database (i.e. database record) but rather deleting the physical location on disk. The system would follow this policy for many reasons including reducing the quantity of the unnecessary stored data by using the

available storage on the server efficiently, minimising privacy issues, and reducing any potential opportunity for the data to be stolen or abused. Furthermore, after taking the final decision by the academic, the system will directly produce a PDF-based report and this effectively is the evidence that can be used more effectively. Moreover, to enhance the system performance and improve its scalability, the system follows many database backup and recovery mechanisms, including Hot (immediate – on demand), Cold (predefined), Partial, and Complete database backup and recovery. The command for partial or entire system database archiving can be sent by the system administrator according to institution's or academic's request, or automatically according to a predefined policy. After every complete database archive process, the system will clear the system database to be used in a more effective manner and ensuring a solid implementation. Generally, these policies are system level features, where there is an administrator in the educational institution (e.g. Plymouth University) who is responsible for installing the software, so it is up to him/her to define what those abilities are.

4.3.2.3 Feature Extraction Engine

As there is no need to provide a real time monitoring, the academic then could check after the e-assessment whether the student has cheated or not. Therefore, as soon as the software interfaces in the Data Collection Engine have captured and stored the students' biometric data in the database via the Communication Engine, the Feature Extraction Engine will implement the next phase, which is extracting all necessary biometric features and removing any erroneous data from the captured samples. As illustrated in Figure 4.6, there is a separated feature extractor agent for each biometric modality which has been captured and stored within the system database.

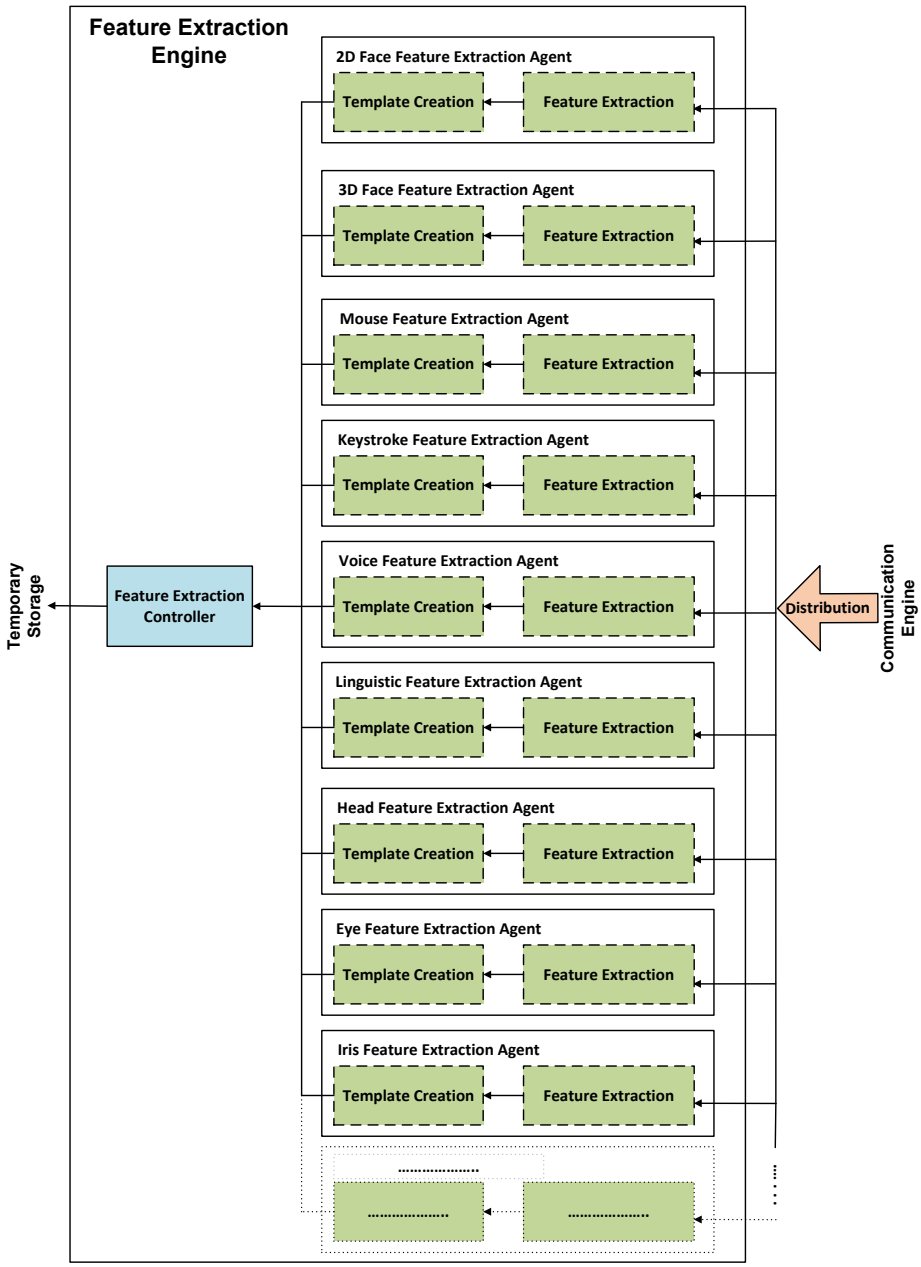
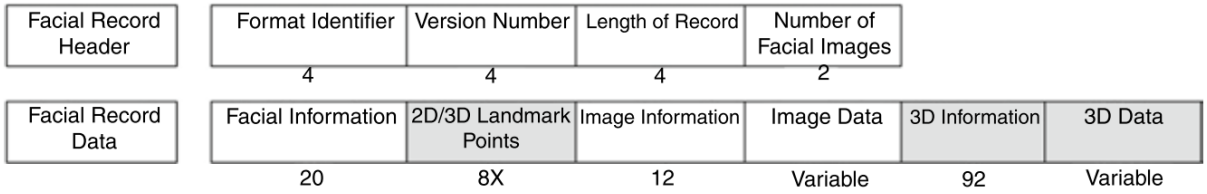


Figure 4.6: Feature Extraction Engine

Therefore, the main responsibility of the Feature Extraction Engine is to extract all these potential features from the processed data and transform this data into a feature vector that encloses the concentrated biometric characteristics to be used effectively for student biometric authentication system. These feature vectors will consecutively be transformed into sample templates in a standard format to be stored in the Temporary Storage by the Feature Extraction Controller. In the student enrolment/re-enrolment stage, the sample template will be used for generating the template, while it will be employed for comparison with a user's profile in the verification process (by the Authentication Engine).

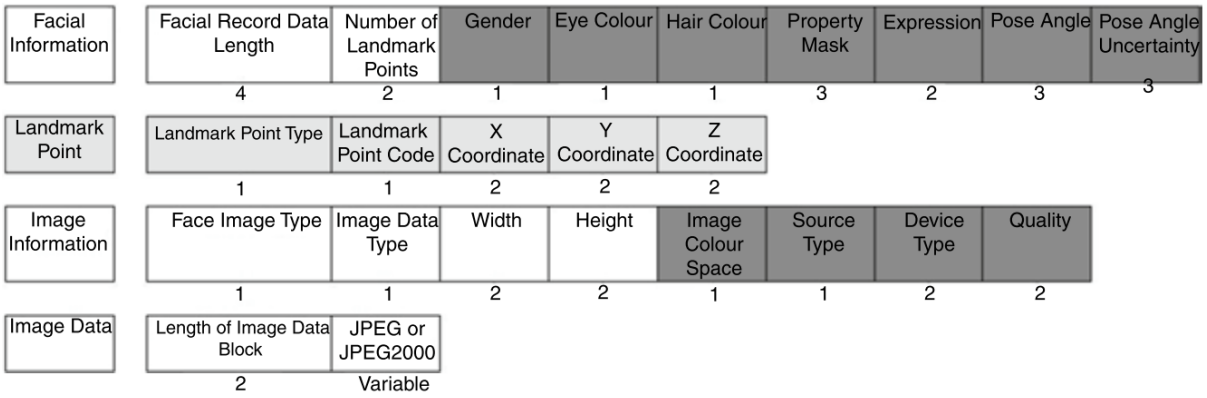
Providing structure and context to the data format enables the rest parts of the system to recognise and interpret the data, eliminating the necessity for individual vendors to develop their own propriety formats, and encouraging interoperability (Clarke, 2011). Therefore, in order to transpose information effectively into the international standard form to enable the plug and play interaction with different modalities, the template that created here will be ISO compliance template. Figure 4.7 demonstrates the face image record format as an example taken from ISO 19794-5 (2009) to provide an understanding of how that template format could look like (whereas each part of the ISO 19794 standard includes a similar method to that of facial recognition, but providing for the nuances required for each modality).



Source: ISO 19794-5, 2009

Figure 4.7: Face Image Record Format

The record format consists of two components: Facial Record Header and Facial Record Data. There can be multiples of the latter but only one of the former. This permits for the communication of various images, through additional record data blocks. The Facial Record Header provides information concerning how many images are present and the total length of the record. The white rectangles of the Record Data block in Figure 4.7 represent the three compulsory blocks that are presented in Figure 4.8, in which provides more details about the content of each section (the numbers below the boxes representing the size in bytes).



Source: ISO 19794-5, 2009

Figure 4.8: Face Image Record Format: Facial Record Data

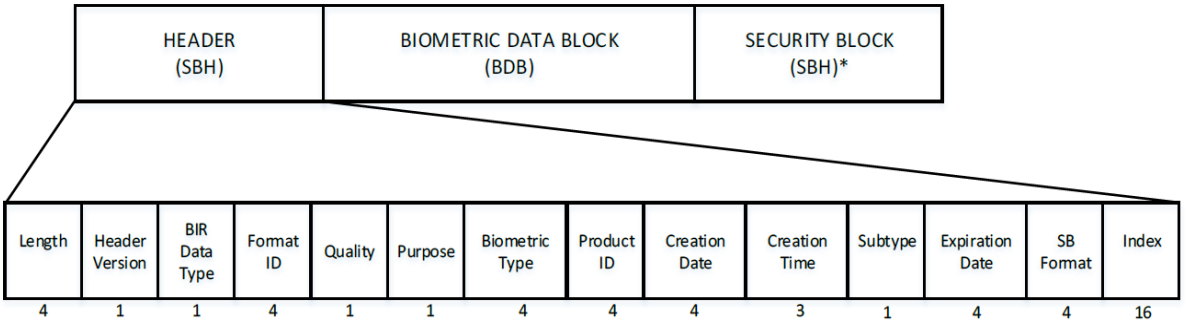
The dark grey rectangles indicate a number of the values that can be unspecified. The Facial Information block contains information about the number of landmark points, gender, eye colour, and pose angle. Information concerning the face image type (basic, frontal, full-frontal), dimensions of the image, sensor type and quality are comprised within the Image Information block. The actual image data is included in the Image Data block. The optional and unspecified parts in this format permit for a greater flexibility in situations where such information is necessary.

The suggested architecture provides the ability to employ single or multi-biometric authentication techniques from a number of biometric vendors (according to the academic configuration utilising the Assessment Manager) during any online assessment. Therefore, in order to guarantee that all these biometric modalities can be utilised at the same time (as long as they are ISO compliance), and their biometric templates can be transferred among the biometric components, the architecture is developed with the relevant ISO standards (ISO/IEC 19794 – biometric data interchange formats, ISO/IEC 19785 – common file frameworks, and ISO/IEC 19784 – biometric application programming interfaces (BioAPI)) in mind. Consequently, the architecture is compatible with these international standards as follows:

The ISO/IEC 19794-1: (2011) is used in order to offer the mechanism for structuring the biometric data into a meaningful form and representation of formats for the interchange of biometric data. It permits three forms of biometric data: raw data, intermediate data and the feature data that can be utilised by the matching phase directly. Employing standardised data interchange formats allows the biometric components to extract the biometric information required.

The ISO/IEC 19785-1: (2015) refers to the Common Biometric Exchange Formats Framework (CBEFF) and is used in order to define a data structure for the exchange of biometric data within the biometric system in a common way. The CBEFF defines structures and data elements for biometric information records (BIRs) for exchanging biometric data. Figure 4.9 shows that the structure of BIR is divided into three parts. The first is the Standard Biometric Header (SBH) contains information about data type and other properties of the Biometric Data Block (BDB) and security options (the meta-information stored on SBH allows the use of templates across different systems). The second part is the BDB contains the actual biometric data in the defined format. And the Security Block (SB) provides

information about algorithms used to secure the record. In order to package multiple biometric samples together, the BIR could have one or more BDBs. Hence, the use of a common data standard allows the components within and between biometric systems to communicate using standardised records.



Source: ISO 19785-1, 2006

Figure 4.9: Biometric Information Record (BIR)

The ISO/IEC 19784-1 (2006) is employed to define an Application Programming Interface (API) and controls interactions between biometric components. This enables the components to communicate, query and execute commands between each other. ISO/IEC 19784-1:2006 covers the basic biometric functions of enrolment, verification and identification, and includes a database interface to allow an application to manage the storage of biometric records. It specifies a biometric data structure which is compatible with ISO/IEC 19785 and 19794. By utilising these standards, the biometric components within the framework are fully interoperable and as such the framework is able to provide a more robust and flexible composite authentication platform.

Due to the fact that the biometric template is a representation of the unique characteristics of an individual, then it considered as privacy-sensitive information. Accordingly, it is crucial to ensure that the biometric information is protected from illegal user access. So, in order to secure the actual information and its transmission, a range of standardised cryptographic-based mechanisms can be used to do that. For instance, all communications between the client and e-invigilation system can be secured utilising TLS, and the database itself can be encrypted through the database management system.

4.3.2.4 Biometric Profile Engine

The key role of the Biometric Profile Engine is to generate variety of biometric profile templates to be utilised consequently by the Authentication Engine for classification – as explained in next the section 4.3.2.5. In order to accomplish this, many template generation algorithms have been employed to take the sample template from the Temporary Storage and produce a unique biometric template. As has been discussed in the previous section 4.3.2.3, the content of each of these biometric templates is different from biometric modality to another. For instance, the template that generated for the 2D Facial Recognition technique could involve a number of distance measurements between key features of a face, whilst the template that generated for the Keystroke Analysis technique could involve a number of weight values corresponding to a trained neural network for the authorised user. The biometric template will be stored within the Profile Storage element by the Biometric Profile Controller, as shown in the following Figure 4.10.

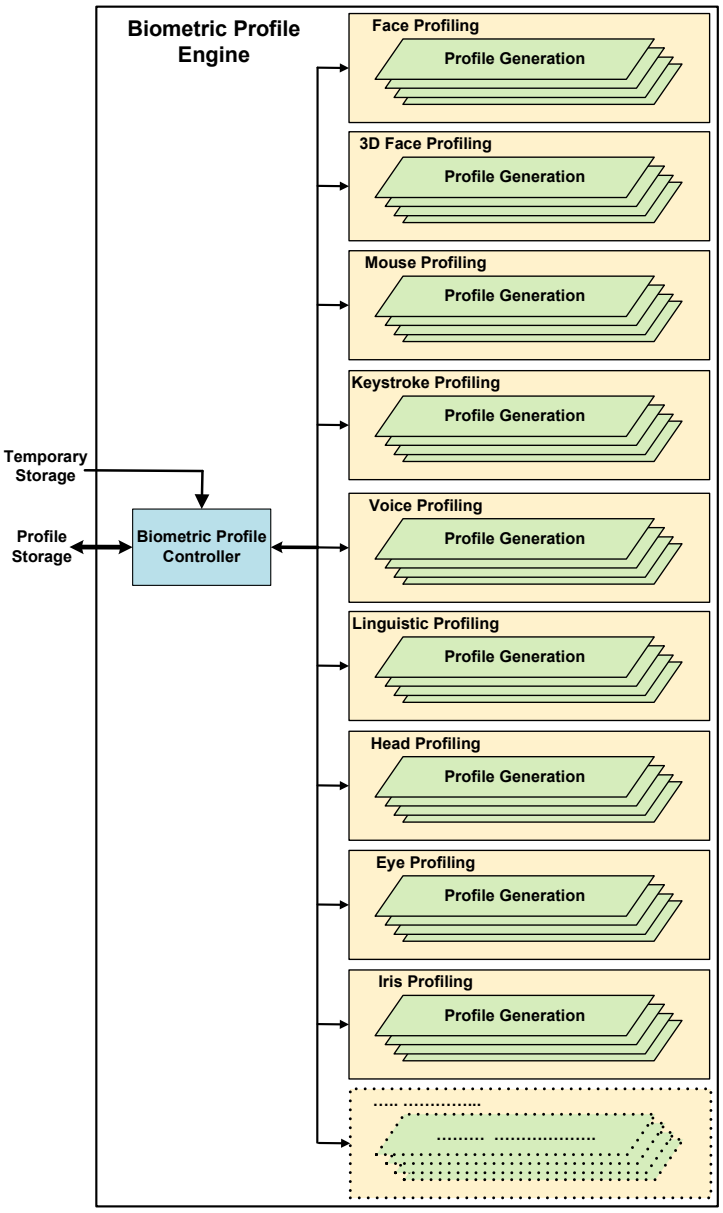


Figure 4.10: Biometric Profile Engine

The system has the potential to utilise many different biometric modalities that subsequently require the student to provide many different enrolment samples in order to generate each initial profile template (at the biometric enrolment stage). This could be a complex process particularly with the behavioural biometric techniques (e.g. keystroke analysis that needs participant training – where the template generation algorithm requires as many as thirty samples before the template can be created) which tend to change over time, therefore, to mitigate this problem and to ensure achieving the required level of accuracy, the system allows the enrolment process to be done through one of the following two ways:

- The student should attend the examination centre in the relevant institution that conducting the online examination, the system administrators, academics, or staff

members then can guide the student to achieve all the required biometric enrolment processes. The identity of the students can be checked in order to guarantee that the enrolled candidate is the legitimate person who will take the test.

- Alternatively, the framework offers the opportunity to achieve a distance- or remote-based but fully controlled and monitored enrolment process, this will be done via the Internet (e.g. over Skype). The system administrators, academics, or staff members then can guide the student to achieve all the required biometric enrolment processes. The identity of the students can also be checked in order to guarantee that the enrolled candidate is the legitimate person who will take the test in future.

Furthermore, as the re-enrolment might be required by the system administrator, the academic, or depending on the predefined periods basis – as sometimes this can be required periodically especially with the behavioural biometric techniques due the fact that they change more often, therefore, as long as the students have done the initial enrolment and taken many e-assessments, a strategy depends on annual basis (e.g. at the end of every academic year) for re-enrolment will be used based on the samples that have been last approved as ligament, these samples can be employed to generate or renew the student's profile template for all the biometrics that have been used.

As shown in the tables below, the Profile Storage element contains variety of the user's input data. There are two kinds of information within the Profile Storage element. The first is a Biometric Template Database (Table 4.4) containing a list of biometric templates that have been generated and file location of the template. In order to implement a full authentication process that will be requested by the academic, this table will be used by both the Biometric Profile Engine and Authentication Engine.

Student ID	ID	Date	Technique	Threshold Scale	Template Storage
1	1	20/08/16	Facial	1	\\profile\template\face1
1	2	25/08/16	Keystroke	1	\\profile\template\keystr..
1	3	26/08/16	Voice	1	\\profile\template\voice
1	4	29/08/16	Mouse	1	\\profile\template\mouse
2	1	20/09/16	Facial	1	\\profile\template\face1
2	2	25/09/16	Keystroke	1	\\profile\template\keystr..
2	3	26/09/16	Voice	1	\\profile\template\voice
2	4	29/09/16	Mouse	1	\\profile\template\mouse
.	.	……..	……..	.	……..

Table 4.4: Biometric Template Database

On the other hand, the second kind of information consists of many tables which hold the raw input data from the student – this raw data (particularly the face images and voice records) could also be utilised as evidence in the Participant Monitoring process. The table contains the file location of the raw data that has been dedicated for each biometric modality. Such as for 2D facial and speaker authentication techniques, the File Location columns determine the path of the physical locations on the disk/server of student's face image, as demonstrated in Table 4.5.

Student ID	ID	Date	Time	File Location
1	1	15/07/16	10:45	\\profile\face\raw1.jpeg
1	2	20/07/16	12:33	\\profile\face\raw1.jpeg
1	3	24/07/16	14:09	\\profile\face\raw1.jpeg
2	1	19/08/16	11:19	\\profile\face\raw1.jpeg
2	2	23/08/16	13:42	\\profile\face\raw1.jpeg
.	.	……..	……	……

Table 4.5: Profile Storage: Facial Recognition

A user's input data is stored even after template generation, as this is required to be used for monitoring and misuse evidence. However, the framework puts a limit on how much data the system wishes to store and for how long. In order to manage this issue, many relevant strategies have been deliberated previously (section 4.3.2.2).

The Biometric Template Database (Table 4.4) also holds threshold data under the Threshold column. This is a numerical scale which provides the system a level of flexibility with regard to the threshold setting of the multi-biometric authentication approaches. As demonstrated in Chapter 3 sections 3.2.5 and 3.2.6, the threshold level defines the level of security that the biometric monitoring system will provide. Increasing the threshold scale would be desirable to accomplish the robustness principle; however, this could also result in frequent rejection of the authorised student increasing the FRR. In contrast, decreasing the threshold scale would reduce the frequent rejection of the authorised student, but this would weaken the level of the security achieved increasing the FAR. Therefore, in practice, this double-edged sword needs to be managed precisely in order to get the best performance. For instance, setting a predefined threshold level of 0.85 might work well for one student but not the others. Consequently, as shown in Table 4.6, the system implements a dynamic scaling for the threshold level which permits the administrator/academic the flexibility to set the threshold based on their preference before any test.

Security Level	Threshold Level
5	High Security
4	Secure
3	Standard
2	Weak
1	Very Weak

Table 4.6: Security/Authentication Level

The administrator/academic then is able to select the desired level of security among five stages: High Security, Secure, Standard, Weak and Very Weak, which represented by the numbers 1, 2, 3, 4 and 5 on the scale respectively. The Standard level will be utilised as the default reference point for the threshold setting of the overall system. At the Standard level, the system threshold for particular assessment is set at the optimum rate which both acceptance and rejection errors are equal (Equal Error Rate or EER). When selecting a higher or lower security level, the threshold will be increased or decreased by x % (where x>0, i.e. 5) of the EER values for all techniques.

However, all the monitoring (continuous identity verification and security) results of every student who has finished the e-assessment will be presented in front of the academic. The system will present/prioritise the students with the greatest percentage of alarms firstly. Although a number of false alarms might be reviewed, the academic still needs to make a decision on all individuals that have been alarmed on the system. Furthermore, the academic also might wish to review none alarmed students, and he/she could change the automatic decision that made by the system no matter it was.

4.3.2.5 Authentication Engine

The main functionality of the Authentication Engine is to implement the student identity verification process. It is this component that has the ability to perform authentication for every permutation of user's input data separately. As shown in Figure 4.11, the Authentication Engine consists of the Authentication Controller and a number of Authentication Agents (it is a variable number and equal to the number of biometric modalities that chosen in the administrative stage), one is dedicated for each biometric technique. The authentication process will be achieved by fetching the required user's input data (sample template from the Temporary Storage) and the corresponding biometric template from the Profile Storage.

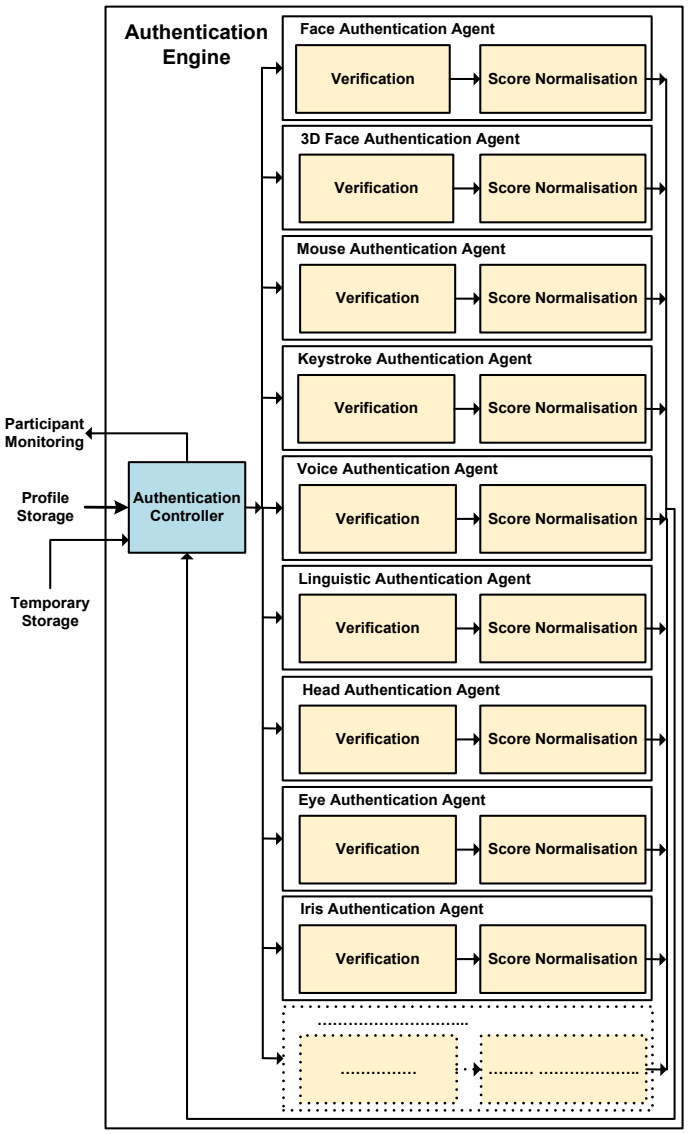


Figure 4.11: Authentication Engine

The Authentication Agent calculates a matching value by comparing the similarity between the sample and biometric profile templates resulting in a matching score. The result of biometric authentication of each individual technique will be compared with a predefined threshold: if the result is less than the threshold, the sample(s) will be assumed to be valid (in this case, the Authentication Controller will send only the taken photo(s) to Participant Monitoring as a valid capture to be reviewed if needed); if the result exceeds the threshold, the sample(s) will be classified as invalid and the Authentication Controller then sends the result of biometric authentication of that individual technique to the Participant Monitoring. Therefore, the raw data in this stage is also necessary, as the Authentication Controller might bring a copy (or the physical location on the system database) of these data to send them along with the authentication result (e.g. in case of authentication failure to present the related instance cases of misuse – as discussed in detail in Chapter 5).

4.3.2.6 Security Monitoring Engine

Whilst the biometric-based approaches provide a basis for continuously verifying the authenticity of the participant, the system has also been hardened to detect misuse and prevent or minimise the opportunity for cheating. The following Figure 4.12 illustrates a detailed Security Monitoring Engine:

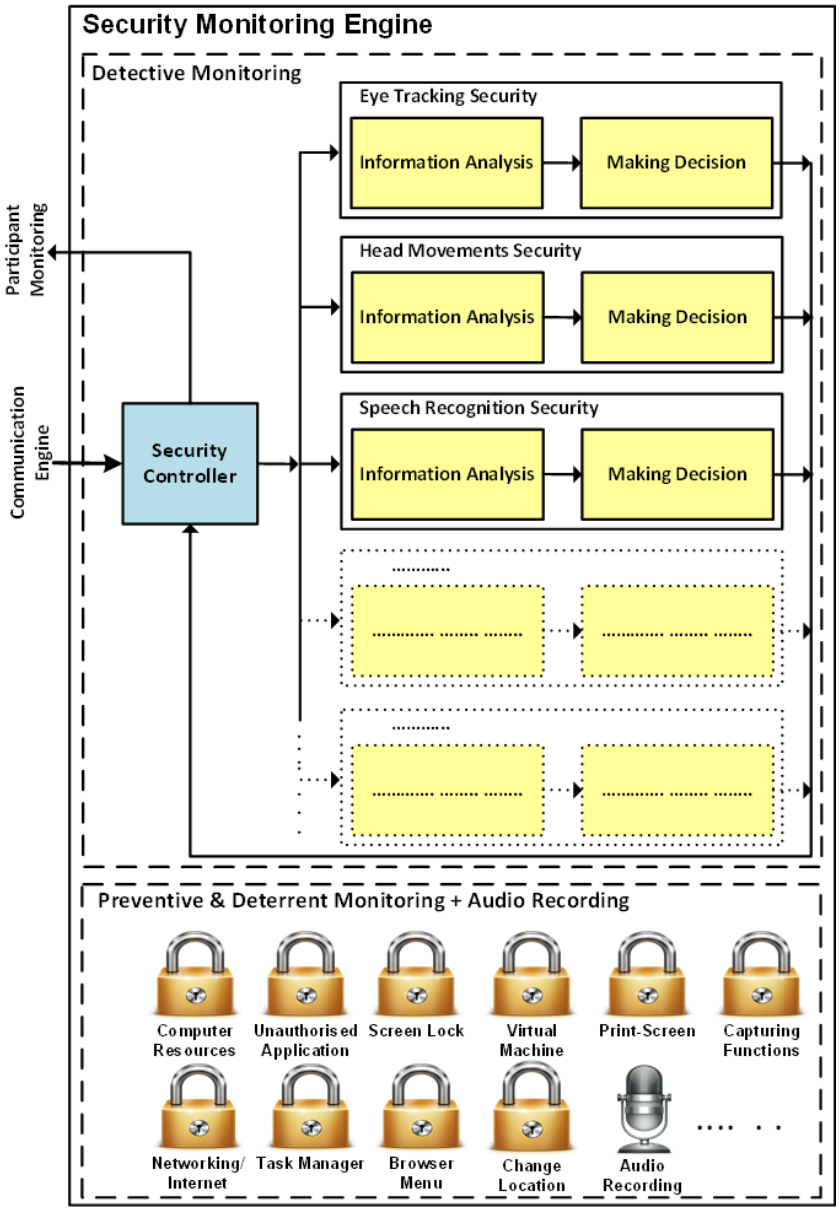


Figure 4.12: Security Monitoring Engine

Analyses of literature (as presented in Chapter 2 – mostly from the commercial solutions) highlighted several areas of opportunity for misuse, therefore, many system security considerations that have been taken into account during the development of EIEA system by preventing test takers from these misuse such as using computer resources, ports, or even the

network including the Internet facilities. These issues are only exasperated by the decision to deploy EIEA within an Internet Browser and further research is required to determine the level of control that a browser can have and what information it is able to provide. Fundamentally, the system security considerations are elaborated as follows:

Continuous misuse detection: All the data of these methods is collected by the Data Collection Engine during the exam time (client-side), the analysing processes however implemented in the server-side. In general, in order to detect cheating, the system could offer the following:

1- The framework could provide a continuous and transparent eye tracking mechanism to ensure that the candidate is looking at the screen (for the majority of the time) that contains the e-assessment without looking at any place in the room or class. The procedure is to take photos (and store them into system database) of the participants whenever their eyes outside the exam screen boundaries for a predefined period of time. The tracking results (the captured photos and all left, right eye movements and centre locations, in addition to the exact time of each of them) a large number of samples every second, that can be tracked, calculated then stored in a text file (in the system database by the data collection engine). All these collected information is required for analysis process by the Eye Tracking security subsystem (as shown in Figure 4.12), the Security Controller then receives the resulted security decisions to send them to the Participant Monitoring to help drawing a complete image of the situation to be reviewed by the academic for taking the final decision, and finally producing a report indicates cases of misuse. Despite the current implementations require a dedicated sensitive near infrared sensor; the new 3D cameras (built in most new laptops) can be also employed for accomplishing the eye tracking process.
2- Supplying a continuous and transparent head movement security. The procedure is to take photos (and store them into system database) of the participant whenever the front of his/her face is outside the predefined angles that must represent the optimum position that the participant's face should be within for a predefined period of time. All the head movements (Roll, Yaw, and Pitch), in addition to all instant time occurrence of each of them, can be measured/recorded continuously during the exam time, and the measurement values/times would be saved in a text file. All these collected information is required for analysis process by the Head Movement security

subsystem, the Security Controller then also receives the final security decisions to send them to the Participant Monitoring.

3- Providing a continuous and transparent speech recognition security. Speech recognition systems provide computers with the ability to listen to user speech and determine what is said. For privacy, avoiding/filtering unnecessary sounds recording, and using the available storage effectively, the framework suggests capturing the human speech then saving it as texts, and recording all times and durations of them. This can be achieved utilising the textual representation of grammars for use in speech recognition. All these collected information is required for analysis process by the Speech Recognition Security subsystem that sends them to Security Controller. The Controller then sends the security decision to the Participant Monitoring in the academic view.
4- Utilising the microphone to record all the sounds in the e-assessment environment to be used as an indicator/evidence in case there is any potential collusion. The complete recording can also be used to clip only the spoken sentences that collected in Speech Recognition security, as the start and end times are also recorded then the exact location and length of the sentence become accessible in order to be utilised for enhancing the monitoring process.

Continuous misuse prevention: All the misuse preventing processes can be accomplished instantly during the exam time, however, the system could send some preventing misuse actions in order to assist the security monitoring and take the best final decision accordingly. For instance, if the student was trying to use virtual machine during the test, then, in addition to preventing him/her from doing this, the system will report this to the Security Monitoring Engine accompanied with a screenshot of the instant desktop indicating a major misuse action. In general, in order to prevent active/motivated/targeted cheating, the framework offers the following:

1- Typically, it is crucial to prevent test takers from reaching computer resources, this is accomplished programmatically by restricting the ability of the student to access any information stored in the computer being used to take the test, the computer ports, secondary storages, intranet network, all wireless connections and even the Internet (Sabbah, 2012).

2- Preventing test takers from accessing any unauthorised application during the e-assessment (Sabbah, 2012).
3- Preventing the ability to minimise, close, and resize the online assessment window (the online exam is locked with a full screen during the whole exam period to prevent the test taker from accessing resources on his/her computer which could contain the exam material or unauthorised helpful information) (Kryterion, 2014b).
4- Inhibiting the ability of printing, Print-Screen/screenshot, screen-sharing, desktop capture, or remote access (Respondus, 2014).
5- Banning test takers from implementing any capturing functions including hot keys, copy, cut and paste (Coursera, 2014).
6- Inhibiting instant messaging to prevent communication with possible illegal assistance.
7- The browser of the system blocks the access to the task manager, disables the launching of scheduled tasks, and prevents the ability to access any other application.
8- Stopping the right-click, function keys, and browser menu (Respondus, 2014).
9- Preventing the ability to run Virtual Machine programs. With the growing number of free Virtual Machine programs, the ability to run the online test in a virtual test represents a big challenge. Therefore, the system always provides an up-to-date mechanism to prevent running them. While running virtual machine is prohibited in many commercial invigilators, based on testing of Securexam, it was determined that it detects virtual machines from VMW and Microsoft Virtual Machine (Percivalet al., 2008).
10- Showing live video stream of the student during the exam as well as a voice recording icon to give the student an indicator that the online test is being invigilated. This might play psychological role to discourage the student from commit cheating.
11- Preventing students from taking the exam at a later date other than the one determined by the responsible academic. Furthermore, the entire e-test ends automatically once the e-assessment predefined time is elapsed.
12- If the student takes test outside the institution, then the exam physical location is supposed to be stable in a predefined location that given by the student, the system will then specify the geolocation of the student (to ensure that there is no possibility that the exam environment has been separated from the monitoring by any mean). This can be done by the GPS of the device, through the Internet connection or even along with every taken photo.

13- Periodical screenshots will be taken to ensure that there is no computer software working in the background implementing any sort of remote control, desktop sharing or file transfer between computers.

Similar to the threshold idea in the biometric authentication the level of security can also be predefined. For instance, the time that the student's eyes can spend outside the screen boundaries, or the values of the angles and times that the student's face should be within the screen before taking a photo; these could be changed according to the academic desire and implemented by the system administrator via manipulating security level of each particular detective security technique. Increasing the security level would be desirable to get a highly secured system; however, this could also result in taking a large number of unrequired photos. In contrast, decreasing the security level would reduce the number of unrequired photos, but it would weaken the level of security achieved. In practice, this double-edged sword needs to be managed accurately in order to get the best performance. For example, the system permits the administrator/academic the flexibility to set the predefined periods of time that the student eyes can spend outside the screen boundaries (in eye tracking security), based on their preference before any test.

Generally, Table 4.7 shows how it is possible to select the desired level of security among three levels: High Security, Secure, and Weaker Security which represented by the numbers 1, 2, and 3 respectively. The secure level, for instance, can be used as the default reference point for the security level setting of the overall system.

Security Level	Threshold Level	Example Set of Functionality
3	High Security	• All biometric modalities that selected by the academic with every 5 seconds capture. • All security tracking with minimum time (every 3 seconds capture). • All the preventive security are required.
2	Secure	• Facial recognition + one of any available biometric modality with every 10 seconds capture. • All security tracking with every 6 seconds capture. • All the preventive security are required.
1	Weaker Security	• Facial recognition with every 15 seconds capture. • Sound recording and speech recognition.

Table 4.7: Selection of the Desired Level of Security

It is the responsibility of the administrator who set the system up to define what functionality will get each level because it is an institutional based functionality in terms of what form of monitoring they want to place. Table 4.7 shows an example of how the nature of the preventative measure and the biometric monitoring can be varied. For instance, by selecting the higher security the system should run all biometric modalities that have been selected by the academic with every 5 seconds capture and every possible tracking being done with minimum time (every 3 seconds capture), this particular level of security would be desirable to be implemented with, for example, very important test which could be a 100% of the module and the academic wishes to make sure that no student can cheat easily and they have to use all the biometrics, the system in this case forces that they cannot sit the test unless their platform has all the required biometric technologies, otherwise they might have to attend the nearest examination centre that could achieve this required level of security.

In more relax situations; the academic can force using the face recognition as mandatory biometrics in addition to any available behavioural or physiological biometrics with every 10 seconds capture, further to all security tracking with every 6 seconds (longer) capture, this level of security might be desirable to be implemented with less important test in which the academic may feel this level of security is sufficient. Therefore, in this case, if the student's system had face and for instance keystrokes or mouse but did not have iris then he could still sit a test. However, the academic could manipulate the threshold setting of the biometric modalities themselves to make it more relax in order to get more capture of potential cheating.

In different scenario, it could be an open book test and no matter if the student surfs the Internet, resizes the e-assessment interface window, or even uses any available materials to assist him/her during the exam time, so the academics do not need to monitor the students with top of detection, they merely looking for basic level of security that would include, for instance, some basic biometric based sampling (e.g. face recognition with every 15 seconds capture to ensure the legitimate student is presence), but there is no need for most system based security such as eye tracking and head movements as the nature of open book test is very deferent from the ordinary test.

Generally, the above security level table is not definitive but flexible/dynamic in which the administrator can add/remove functionalities or security levels according to the institutional requirements.

4.3.2.7 Communication Engine

The Communication Engine provides a communication interface between the stored data and the online system framework. Using the available attached/built-in devices, the machine that used for conducting the e-assessment is responsible for capturing the biometric and security input data of the student (involving the Data Collection Engine) and then sends this captured data to the Communication Engine for storing them safely into the system database (e.g. servers). The role of the Communication Engine is to transfer information based upon 5 categories, as demonstrated in Figure 4.13.

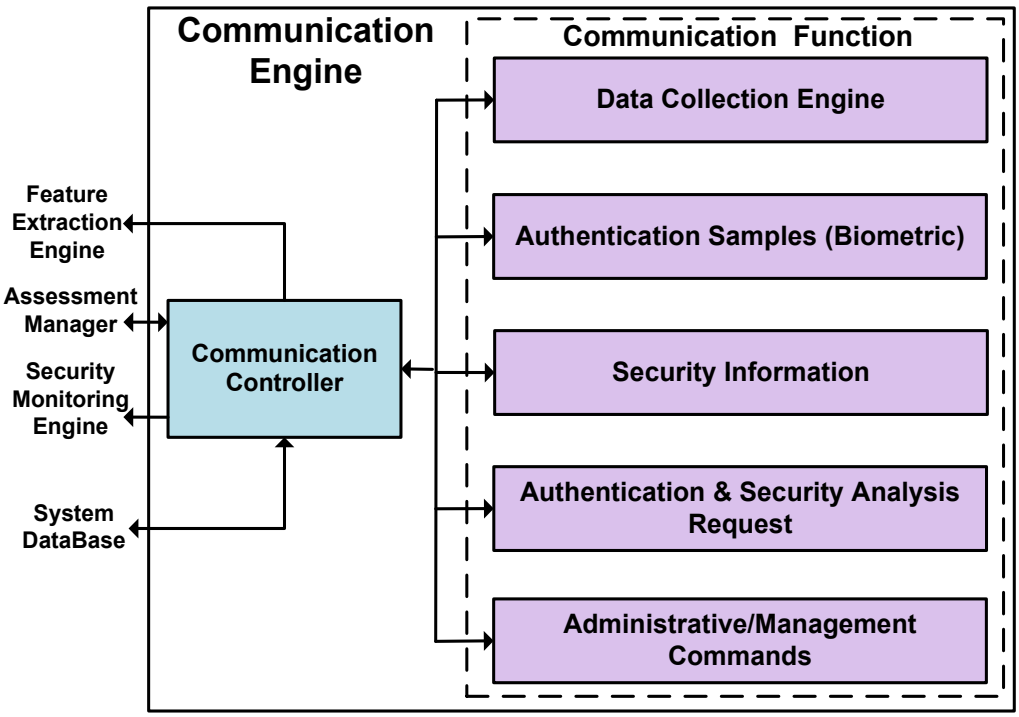


Figure 4.13: Communication Engine

Once the authentication input data is stored, it will be retrieved by the Communication Engine to be submitted to the Feature Extraction Engine, and the stored continuous security detection input data will also be retrieved by the Communication Engine to be submitted to the Security Engine. The communication engine works as a bridge between the captured biometric and security input and the framework. The Communications Engine also enables the Assessment Manager to send some high level commands to the student (e.g. orders for performing re-enrolment), the academic (e.g. the need for archiving the entire system database), or implementing the periodical predefined operations (e.g. implementing automatic

partial/complete (hot or cold) backup operations to the entire system database periodically in order to improve the system performance).

4.3.2.8 Assessment Manager

The primary role of the Assessment Manager is to enable the user to achieve a variety of management-level functionalities that provide the basis for creating and managing assessments. There are different views of the system are provided to the stakeholder users (i.e. academics and students); however, wider administrative authorities and grants are given to the inspector over the student. As illustrated in Figure 4.14, further to the high level administrative abilities, utilising these user-friendly interfaces, the academic can create and define an exam, view or edit existing exams (Create, Delete & Edit Exam), review the authentication and security results to make the final decision through the ability to confirm or deny cheating (Participant Monitoring). The student, on the other hand, can view and take available exams (View & Take Exam), in addition to enrol or re-enrol the biometric modalities under the supervision of the academic or staff member (more details about the practical implementation of these are shown in the next chapter). The system could automatically send emails to the academics, alarming information, or warning messages to the students as part of the preventive security subsystem (if necessary).

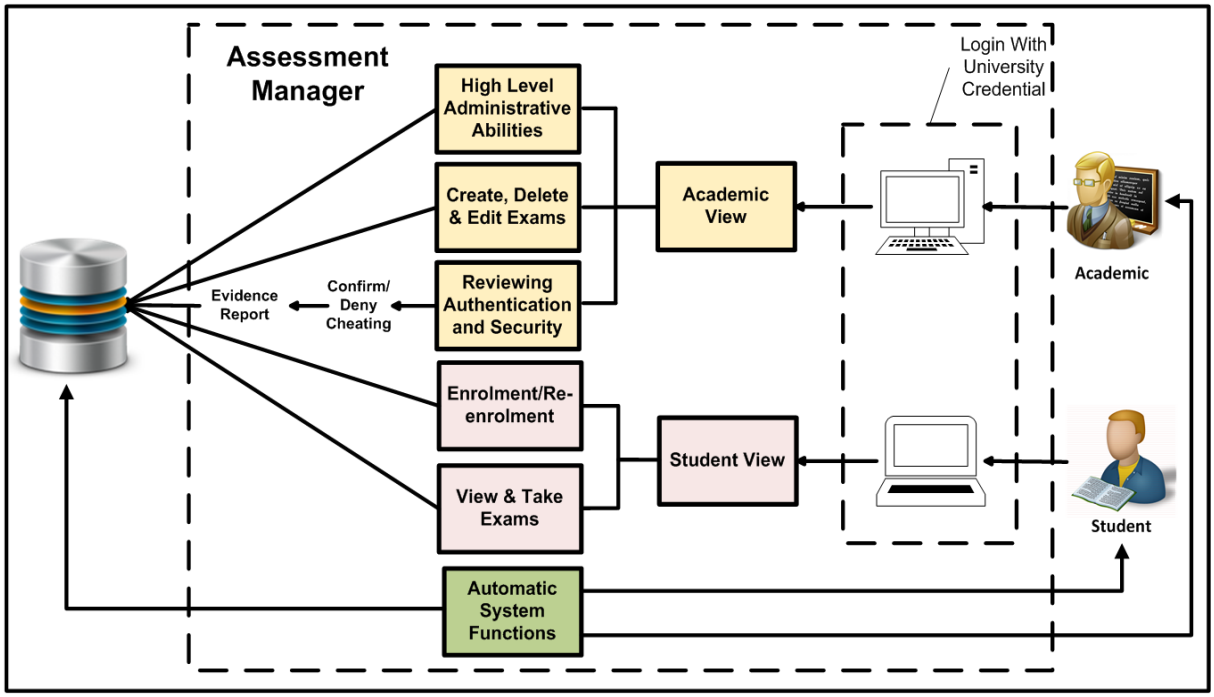


Figure 4.14: Assessment Manager

In general, the following Table 4.8 demonstrates the high and low level administrative or management abilities/activates that can be accomplished by each of administrator, academic and student.

Task or Functionality	Administrator	Academic	Student
Defining and adding/removing authentication techniques	✓	X	X
Defining and installing/uninstalling compatible software/SDKs	✓	X	X
Defining the maximum number of concurrent examinations (at the same time)	✓	X	X
Defining and adding/removing security approaches	✓	X	X
Creating new test	X	✓	X
Editing/Deleting test	X	✓	X
Review taken tests	X	✓	X
Review authentication and security results	X	✓	X
Denying or confirming cheating	X	✓	X
Creating/Providing reports of cheating as accessible evidence	X	✓	X
Defining and adding/removing compatible hardware devices	X	✓	✓
Supervised biometric enrolment/re-enrolment	X	X	✓
Security calibration	X	X	✓
View available tests	X	X	✓
Take available tests	X	X	✓

Table 4.8: High and Low Level Administrative/Management Abilities

Generally, depending on the available infrastructure, the system also provide the administrator the ability to define the maximum number of students that complete assessment at any point in time, and then when setting up a new assessment the system does a check at that point in time to make sure that tests number available for students does not exceed maximum number before allowing an academic to actually set that particular test. For instance, an academic cannot schedule a 2 o'clock test if there are already tests scheduled for more than N number (N > maximum number that was defined by the administrator) of individuals, as basically that particular time just has not been available, this policy has been followed just to ensure the system is never scheduled at a point where it is going to have oversupply of people want to sit assessment that would break the infrastructure.

4.4 Real-Time Processing/Scenario

The architecture was developed with non-real time processing in mind because there was no need in the requirement to provide a real time monitoring, so the academic can check after the exam whether the student has cheated or not, as there is no need to do that check in real time. However, should there is a need to be real time analysis, as essentially, for instance, the typical use of assessment platforms tend to be focused around few weeks each semester when the students take the assessment (i.e. at the end of the semester), therefore, when there are thousands of people want using the platform all at the same time, in this case the architecture does not need a change but the platform and system that it sits on will need to be properly designed to be elastic in order to allow for vast increases in computation in order to cope with that real time aspect. Hence, to enable this real time process, the system requires an elastic platform where, for instance, the biometric processing engines run on ten rather than only one machine. Furthermore, to gain a more processing and computation ability, the database also might need to be a multiple platform database management systems split across multiple servers. Therefore, similar to the interaction in general architecture in section 4.3, Figure 4.15 presents an illustration of how the interaction would occur between the client and the server in real time processing, the architecture still has the same components but now it has been distributed and load balanced on the infrastructure. The load balancing is required to make sure the signals easily get spread between the multiple services. One potential way to achieve/provide the aforementioned infrastructure is by utilising cloud computing platform to allow for a vast increase in the capacity that might be required over small durations of exam periods.

On the other side, even under the non-real time processing scenario, the system probably still needs that kind of elastic platform which allows for vast increases in computation, for instance, the batch process of 10,000 people all sat one e-assessment could take very long time (e.g. two weeks), because the architecture is run on one server, so in terms of scalability aspect as well as real time processing, the system needs to increase and reduce the processing backend accordingly (providing the elastic capacity when required).

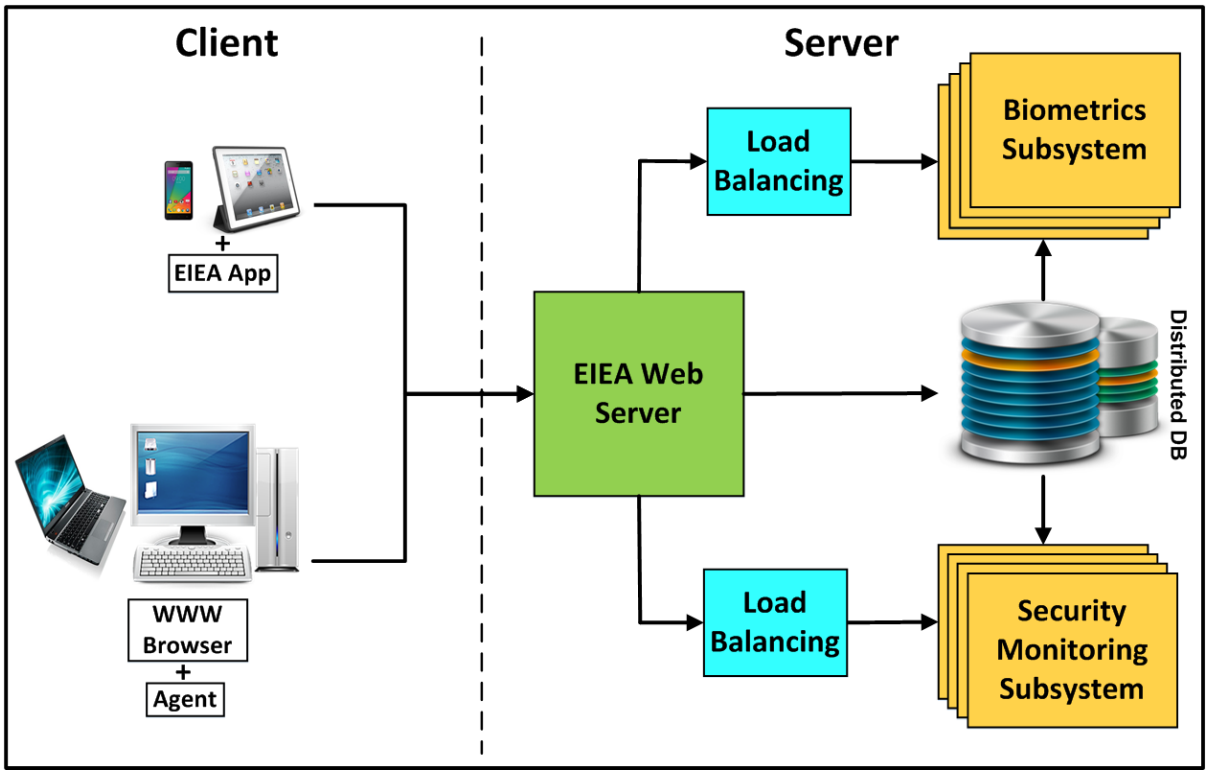


Figure 4.15: Real-Time Interaction between the Client and the Server in EIEA

4.5 EIEA System Processes

As shown in Figure 4.16 (the complete EIEA system processes), there is no need for point-of-entry access authentication because the system will utilise the hosting organisation authentication mechanisms (e.g. Shibboleth single sign-on). In the e-invigilated e-assessment environment, the academic can implement many activities including but not limited to creating assessment with details to be stored in the system database, in addition to monitor and review student activities during the e-test to review any possible alerts.

From a student perspective, the system will have to support the enrolment process, in order to build the biometric profiles to be stored in the system database for the purpose of continuous verification. This can be acquired by matching the captured data during a monitored test against the stored templates. Furthermore, the student enrolment should be controlled by the academics; the student should provide all the required biometrics in this stage in order to be able to take any test among the list of the available (in particular period of time) tests.

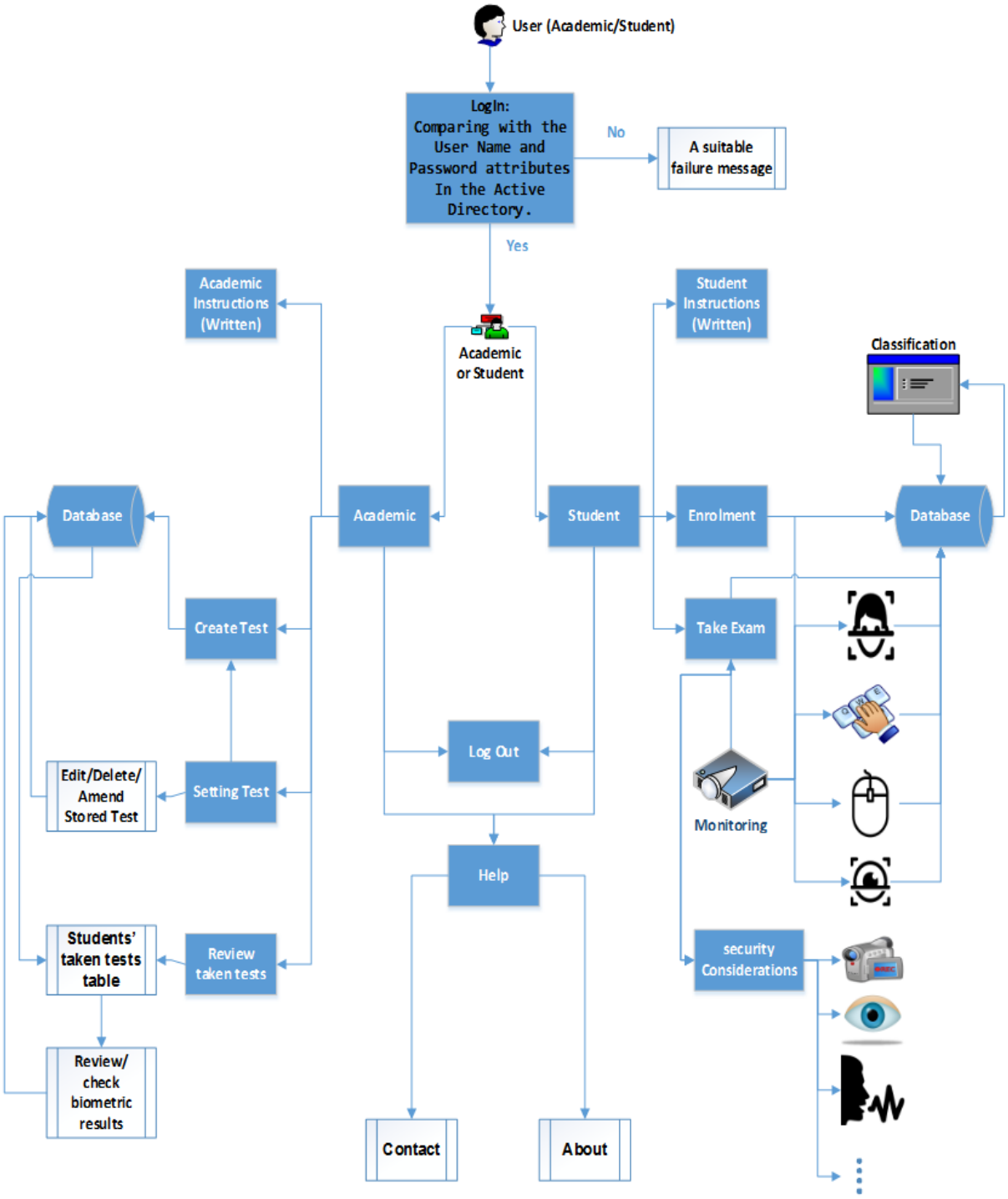


Figure 4.16: System Processes Diagram

Once the user (academic or student) has logged in, the system will then automatically direct him/her to the required subsystem (either to the academic or student subsystem). Some tabs and sub-tabs in the main system interface are shared between both academics and students, such as: Log Out or Help; others are dedicated for the two roles. Both are required to follow predefined system instructions. The academic has the ability to create new tests, edit, delete, or amend any stored or available test and to review/check students that have taken tests and

their biometrics and security results. The principle of transparent or non-intrusive monitoring has been implemented in a fully controlled e-assessment environment. While the student biometrics are stored to be compared later on, the biometrics and security monitoring are continuously in operation. The system could also provide variety of instant messages, for instance, to clarify cases of failure for some process (e.g. providing invalid date and time in test creation).

In test creation process, the academics need to provide names for each test to differentiate between their tests. The date, time and duration are also essential. The academic has a full control over his/her created tested, they can amend the created test settings such as changing the dates and names or even deleting, these can be accomplished utilising many of user-friendly management interfaces that could also offer fast access for the available tests and all the results of the achieved monitoring process.

4.6 Discussion

Generally, in the online assessment environment, the system can face many challenges; some of them are general and can be controlled in the same way the traditional examinations would deal with such as people health, cultural, religious or even technological problems. Some people might suffer from health problems such as eyes/sight permanent problems (e.g. blindness, or cross-eyed), these particular cases, as with the traditional examinations, should be managed by providing special cases that the institution can specify to make the online examination possible and secure at the same time, the solution could involve exclusion of some biometric modalities and security restrictions (e.g. iris recognition, eye movements or eye tracking security). Furthermore, as the online examinations are supposed to be implemented on a global basis, so, there are numerous cultures such system should be fixable and could adapt to deal with them. For instance, some cultures insist that the women must wear the face veils, in this case the exclusion may include the essential biometric modality (i.e. face recognition) rather than secondary, the alternative here should be a range/combination of solid biometric modalities (e.g. iris recognition) in addition to other behavioural biometrics (e.g. mouse dynamics, keystroke analysis, eye movements, or head movements).

On the other side, some challenges related to the student ability to always inventing a new way for cheating, for instance using a small earphone to hear the answers by somebody else

outside the room. It is very difficult to read the question in front of the examinee during the test by anybody else without catching him by the camera. Even though they could access the question somehow, the problem can be solved by asking the student to show his/her ears to the camera before the start of the exam in order to take photos of them to ensure there is no earphone in there. Fortunately, these photos also might be utilised for ear recognition of the student identification in the log in process providing additional robust and transparent biometric method.

Furthermore, a typical problem would be related to the nature of the exam itself, for example, some exams might include particular questions that might need relatively long time and/or calculations to be solved, this would require using pen and paper apart of the computer/machine being used to achieve the e-assessment, or access some resources on or out the computer, in this case, when defining the exam questions, there is ability to highlight a specific question and turn off the eye tracking ability while answering this sort of highlighted questions as might be additional work is required, therefore, there is expectation for user's eyes to probably move from the screen, and in this case this strategy does not allow the system to flag misuse.

4.7 Conclusion

The development of a secure invigilation for e-assessments, capable of exceeding the key limitations in e-learning (the cheating problem) has addressed the requirement of advanced authentication and security mechanisms. Therefore, this novel e-invigilation system is designed in a modular fashion to incorporate a range of behavioural and physiological biometrics (the most user-friendly and robust techniques) and system level security. As the use of a composite authentication approach provides a robust and transparent method of increasing authentication security beyond traditional point-of-entry systems. The level of authentication security is, however, dependent upon the user (academic) need and the authentication techniques that are available/involved during the test. The architecture has been designed around two operational objectives: continuous biometric-based monitoring of the participant and system-level monitoring to detect and prevent cheating. Furthermore, it provides a variety of management-level functionalities for creating and managing assessments. The key to user acceptance is usability and the system has been designed to specifically ensure ease of use for all users (i.e. academics and students). Therefore, the users can benefit from the system in terms of both exam security and convenience of use.

Although the previous research in the area of invigilation shows some endeavours to involve biometric authentication for securing e-assessments, none, however, have developed an architecture that capable of dynamically adjusting to the wide range of techniques, as a system that is flexible to enable it to adapt to new monitoring and biometric technologies. Furthermore, none of them provides academics with prioritised and usable interfaces to verify and check cases of possible cheating.

5 EIEA Prototype

5.1 Introduction

In order to highlight the ease of use and lightweight nature of the system, a prototype of the previous architecture in Chapter 4 was developed. Therefore, this chapter presents, in detail, the development and implementation of an EIEA prototype from the two perspectives of the key stakeholders (i.e. academic and student). Given the flexibility of the aforementioned architecture, a number of decisions had to be made concerning which the most transparent and robust biometric modality to be used in order to provide a sufficient continuous identity verification, what effective security approaches were to be applied/developed, and how to employ the most efficient software/hardware to achieve the targeted level of secure e-examination and controlled monitoring. Essentially, the intention of the prototype in this phase is to perform the validation of the concept of the model. The prototype was developed not to be a complete operational prototype or to implement full commercial operational system but to provide sufficient functionality in order to address the research questions that will be identified in the following chapter. Therefore, in order to monitor the exam taker and ensure that only the legitimate student is taking the exam, the system offers a continuous user identity verification employing facial recognition biometrics; a security layer including an eye tracker to follow/record the student's eye movement, speech recognition to detect inappropriate communication, continuous head movements tracking to check whether they were focusing on the computer screen, and multiple face detection.

At each stage of system development, a series of pilot trials have been conducted within the CSCAN research centre (Plymouth University) and have been developed to ascertain the effectiveness of the technique. It has been implemented as identified in Chapter 4, in which both academic and student will communicate with a central web service (utilising a server-side topology). From a software perspective, there are five different programing techniques have been used to develop the E-Invigilation of E-Assessments prototype, all of them are under the Visual Studio environment including: C#, HTML5, JavaScript, JQuery, and SQL Server, as well as the use of Eye tribe SDKs for eye tracking security via following and recording the student's eye movement, Intel RealSense SDKs for the compassion between the stored biometric profile of the candidate with his/her online exam captured image to obtain the biometric score, and Java Speech Grammar Format (JSGF) for speech recognition.

5.2 Database Implementation

The following Figure 5.1 represents the implementation of system database showing all the linked tables that form the database of the suggested architecture (using Microsoft SQL Server Database). However, when it comes to implementation, additional functionalities would be required in the prototype, therefore, this database also includes some additional tables aligned for the modalities and technologies that have been used in this particular implementation. For instance, FaceExpression table was created to be utilised for managing the various types of user face expressions during the test for different security monitoring purposes. Furthermore, the issues table is added for recording all types of misuse that would be done by the student during the test. Speechjsgf is also additional table that has been created to manage the proposed speech recognition mechanism as one of the security approaches provided by the system.

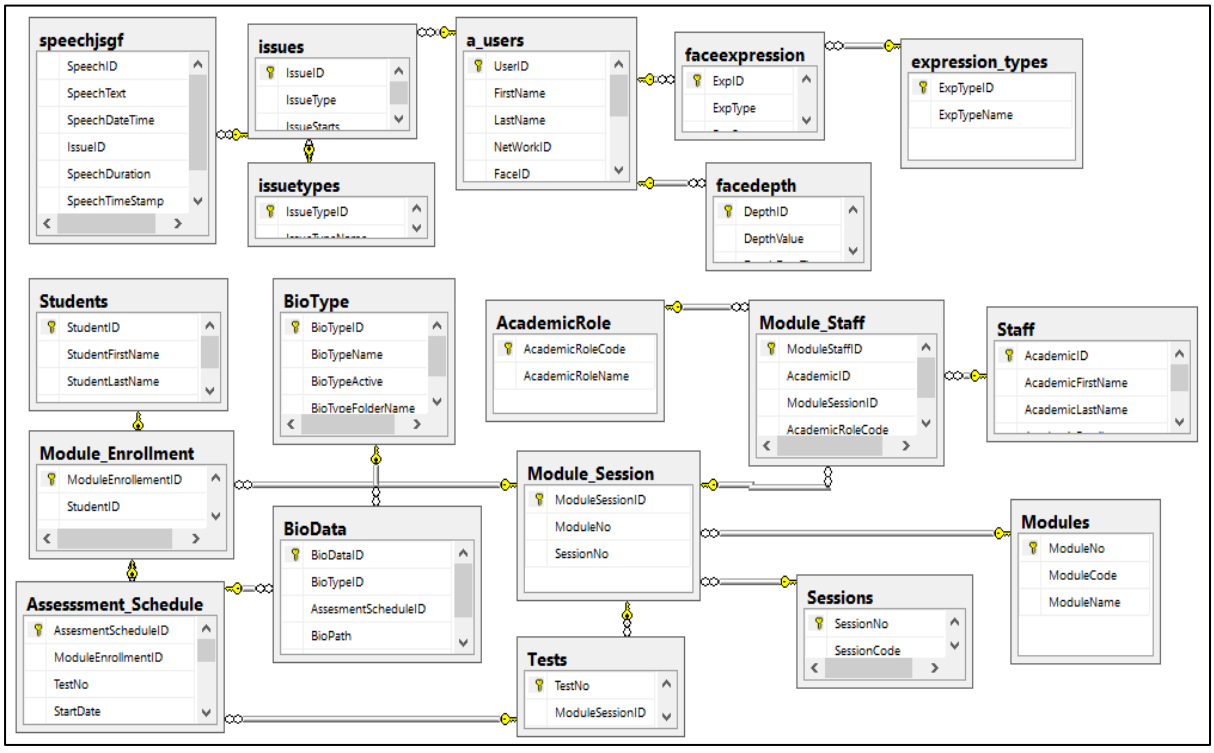


Figure 5.1: The Complete Developed System Database

5.3 System Implementation

The subsequent sections will describe and present the operation of the prototype with respect to the two key roles: academic and student.

5.3.1 Academic Perspective

As discussed in the previous chapter, the academic can accomplish many low and high level administrative management abilities such as: create and schedule exams or view invigilation results and data.

5.3.1.1 Login

This particular setup of the model has been developed with the internal systems of the researcher's institution in mind. The authentication process to access the system is dealt with by central systems via federated identity; therefore, there is no need for a registration process in the academic system.

After entering his/her username and password (as shown in Figure 5.2), each academic will be recognised according to the information in the directory entry and redirected to the system main page.

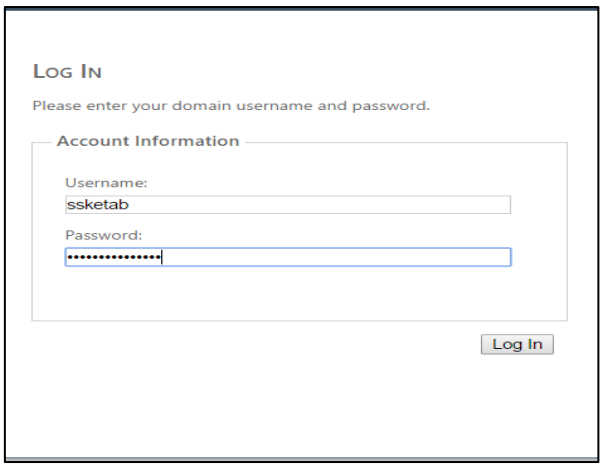


Figure 5.2: Academic Login

5.3.1.2 Academic View Main Tabs

Once the academic logged in there are five tabs available as shown in Figure 5.3, the first tab from the left side of the menu bar contains the system general rules, then two tabs provide the ability to create and view an exam, and the last one for help which includes further sub tabs (About and Contact), in addition to the logout link to provide the ability to log the academic out.

Figure 5.3: Academic Subsystem Main Tabs

5.3.1.2.1 Academic Instructions

Even though it is a simplified, user-friendly, and clear web page with good HCI principles including: (Visibility of system status, Match between system and the real world, User control and freedom, Consistency and standards, Error prevention, Flexibility and efficiency of use, Aesthetic and minimalist design, Diagnose and recover from errors, and Help and documentation), as illustrated in Figure 5.4, there are many instructions that the academic should read before utilising the system especially if he/she uses it for the first time, the instructions can be seen by the academics in the Academic Instruction tab. Also, there are many illustrative messages have been provided in order to describe some unforeseen situations.

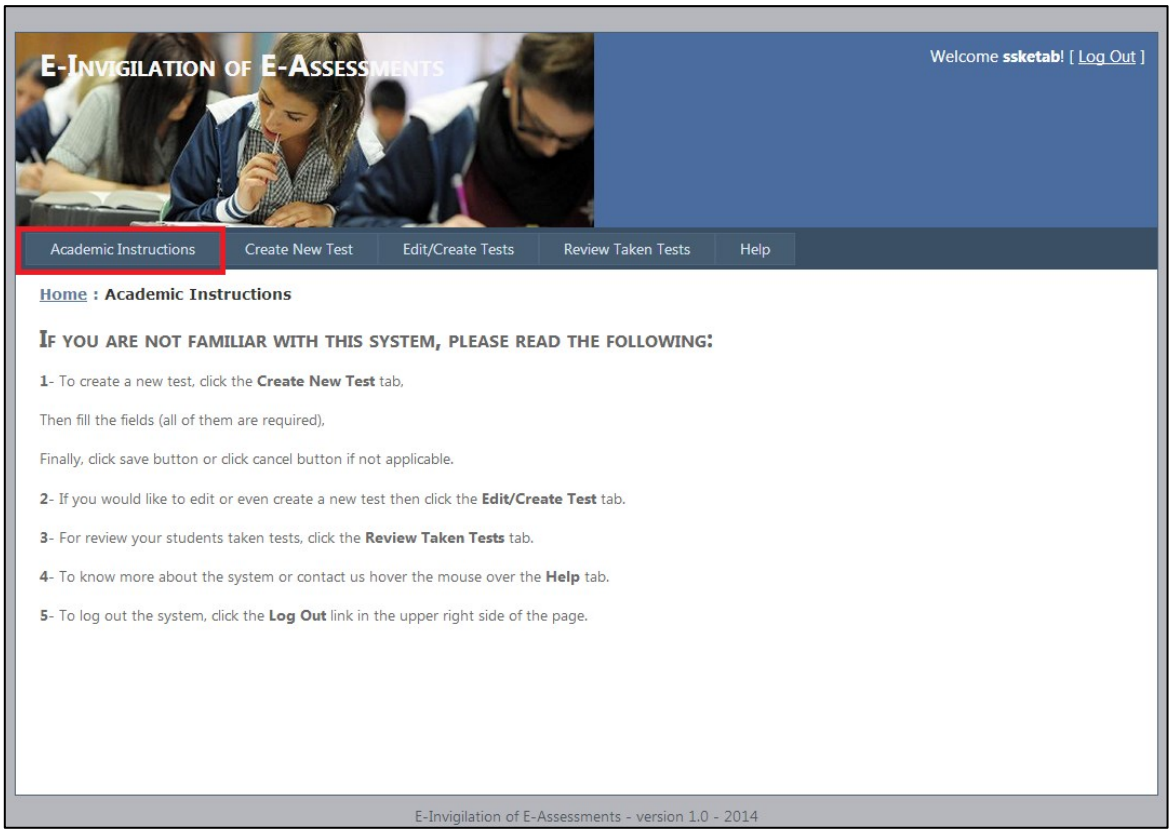


Figure 5.4: Academic Instructions

5.3.1.2.2 Create Test

There is an appropriate page that enables the academic to create and define an exam, view, or even edit existing exams. To create an exam, the lecturer must complete the fields as shown in Figure 5.5. The academic uses a name to differentiate between his/her tests – typically the module/assessment title. The start and end time and duration can be used to enable the academic to either restrict a student from taking an exam until a predefined slot, or alternatively, the academic can set this up so that the student is able to undertake the exam at any point between the two dates.

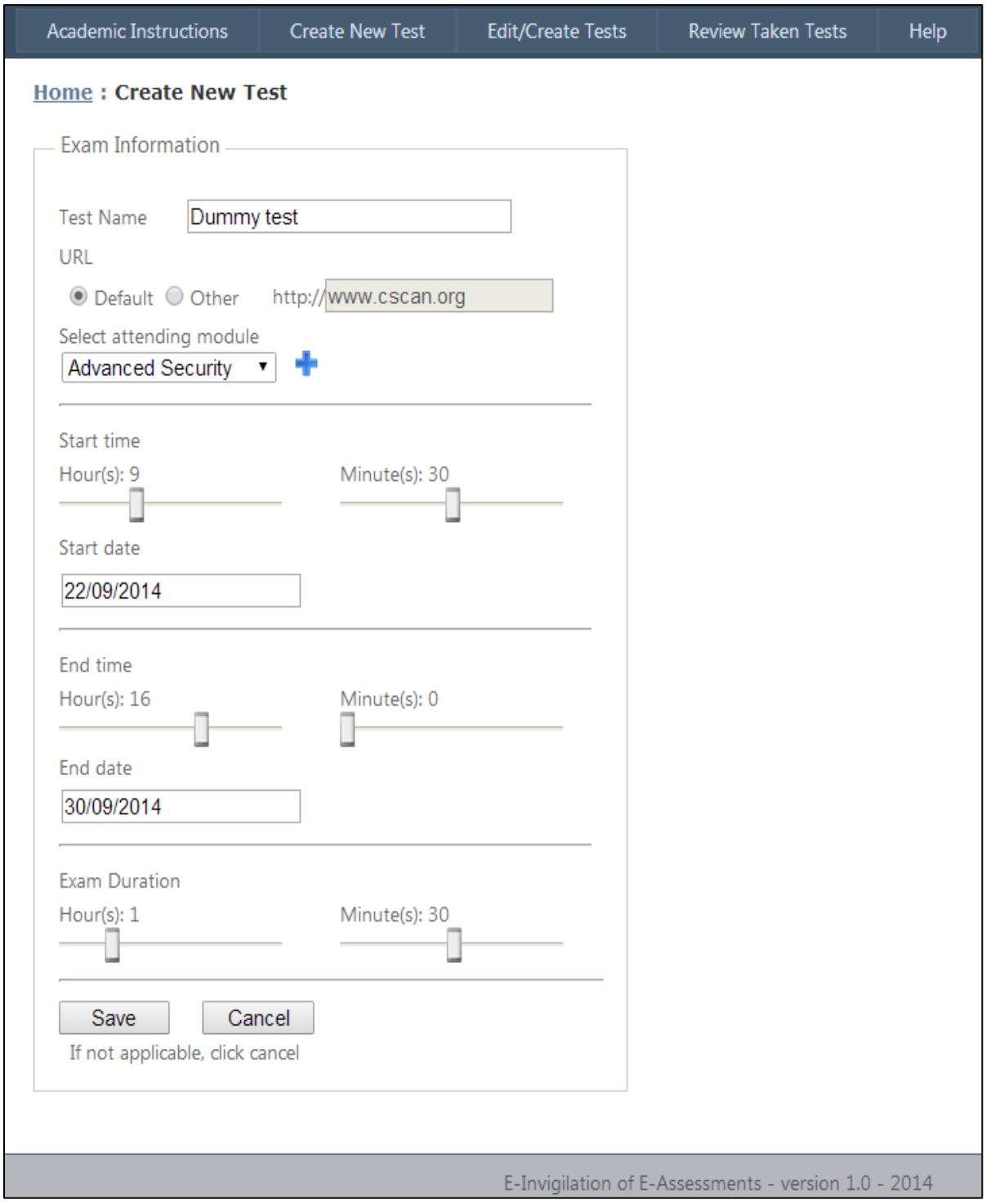


Figure 5.5: Create New Test Tab

5.3.1.2.3 Edit Test

If the academic would like to edit, delete or even create a new test then he/she could click the Edit/Create Test tab (Figure 5.3), this will lead to view a page as illustrated in the following Figure 5.6:

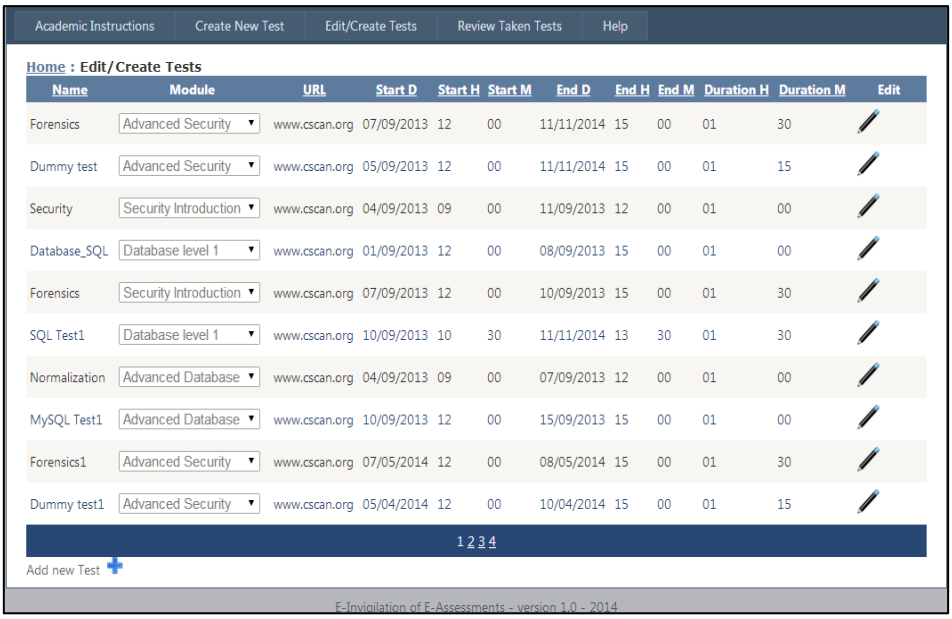


Figure 5.6: Edit/Create Tests Tab

The academic can create edit/delete tests through this page by clicking the pencil icon beside each of the created tests and this will lead the academic into further inner process that requires recalling the same test creation page with the last setting as shown in the following Figure 5.7.

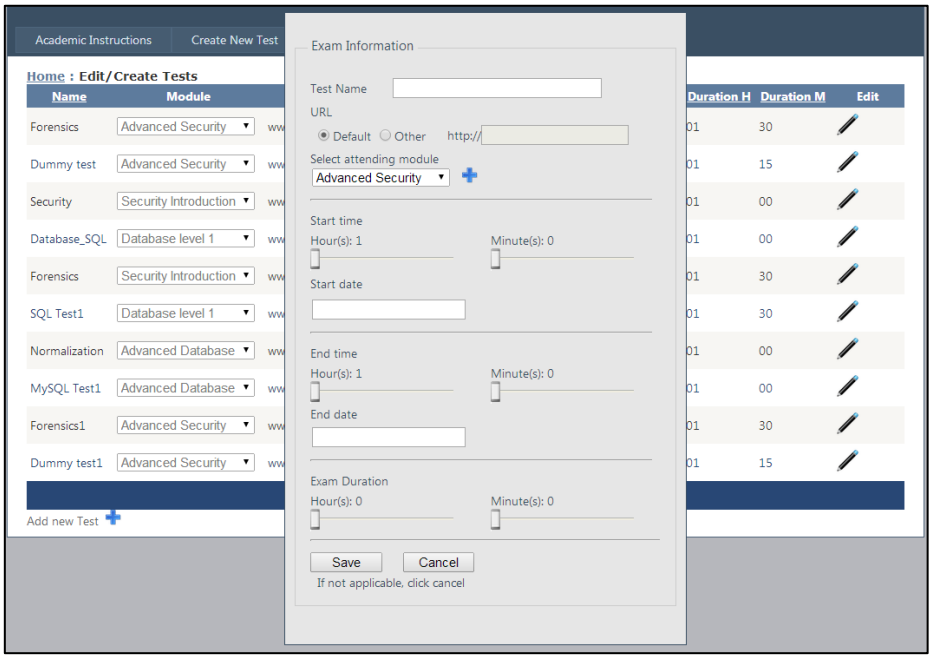


Figure 5.7: Editing Test Process

The academic also can create new test through this page by clicking the blue cross in the bottom of created tests table beside the (Add New Test) test, this will lead the academic to inner process similar to creation new test page.

5.3.1.2.4 **Review Taken Tests**

A management interface is provided to the academic, when clicking Review Taken Tests tab (Figure 5.3), in order to aid the examiner in understanding, managing and accessing their assessments, obtaining an overview of all current and previous assessments that have been defined during any particular academic year, and review/check the biometric and security results of each student as shown in Figure 5.9.

In order to ensure the applicability, usability, reliability and flexibility of these novel e-invigilation system interfaces, they are designed in modular and user-friendly fashion that enables the end user to easily access and retrieve the required data. The most required data in this stage is the facial images and sound files. Particularly, these two data types are necessary to be retrieved in order to achieve the participant monitoring process for both authentication and security purposes. The result of biometric identity verification of each facial recognition technique can be used to compare them with the predefined threshold as discussed in the previous chapter. Copies of the raw data in this stage are also necessary to be used for presentation/evidence purposes. In the authentication part of the framework, this raw data would be a set of images, sound clips, text, or parameter values, whilst in the system security part it could be images, audio files, text, or parameter values/locations for eye/head movements; all together will be valuable for constructing the ultimate e-assessment security decision and documenting accessible evidence.

Therefore, as depicted in Figure 5.8, if the academic would like to show the results of the invigilation of particular student, he/she simply can click the *Show Authentication Results* tab in the main interface, then must choose each of the *Module Name, Session Number, Test Name,* and *Student Name* respectively, and finally, click *View Result* button.

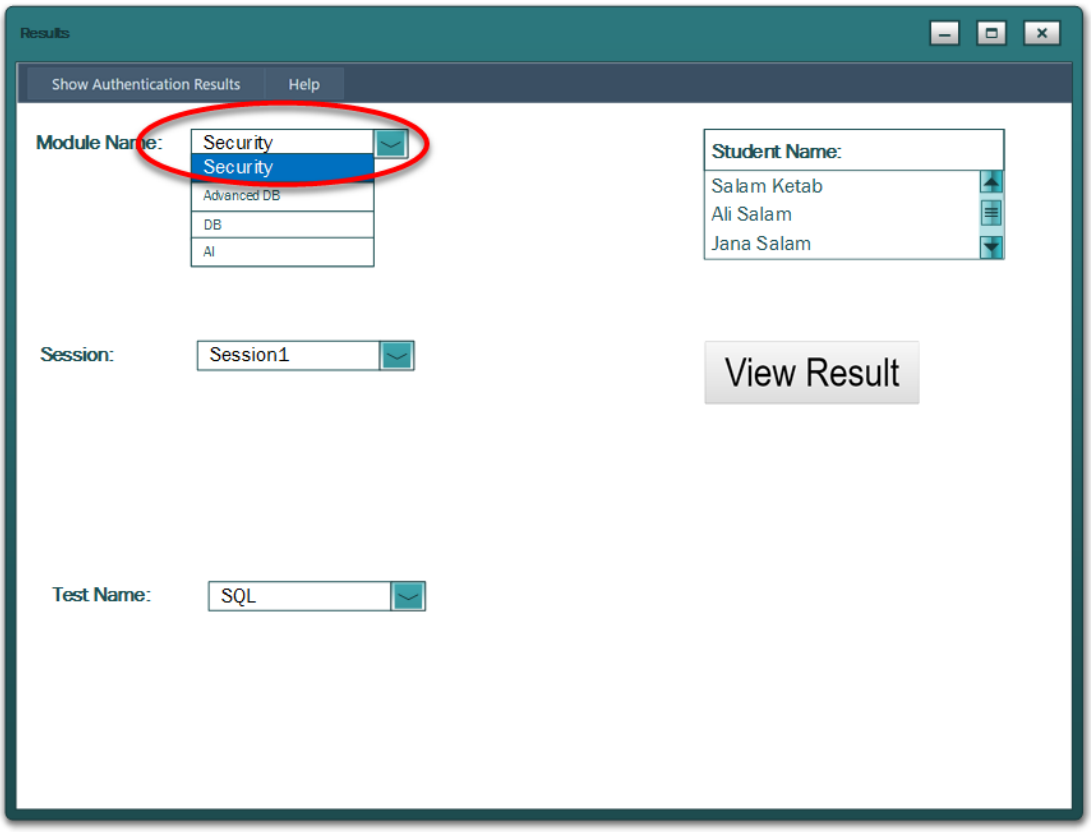


Figure 5.8: Result of Student Selection

Each of the above selected information was fetched from the stored system database that has been initiated by the academic, as illustrated in Table 5.1, during the creation of the assessment process.

Test ID	Module ID	Session ID	Test Name	Test URL	……..
1	1	2	Forensics	www.cscan.org	……..
2	1	3	Dummy test	www.cscan.org	……..
3	2	1	Security	www.cscan.org	……..
4	3	2	Database SQL	www.cscan.org	……..
5	2	1	Forensics	www.cscan.org	……..
6	3	1	SQL Test1	www.cscan.org	……..
7	4	4	Normalization	www.cscan.org	……..
8	4	2	MySQL Test1	www.cscan.org	……..
9	1	3	Forensics1	www.cscan.org	……..
10	1	1	Dummy test1	www.cscan.org	……..
.	.	.	.	.	……..

Table 5.1: Tests Table

The system will then show another interface (Figure 5.9) to present the authentication and security results. These interfaces have been designed to enable the academic to review the

alerting images sufficiently in order to allow him/her to quickly identify and judge cases of misuse happed. This particularly important when they got large volume of classes, the key at this solutions that most misuse identification in the identified approaches in prior literature are relying on reviewing the results of video monitoring, the problem with this method that the academic needs to watch, for instance, in minimum a 30 minutes of video for 200 people, while this is about detecting people doing misuse and highlighting them as quickly as possible to save the academic having a review and spend hours merely seeking for the misuse himself, in this case, he/she will act as a physical invigilator. Therefore, it is an essential job to provide interfaces that allow finding and identifying the individuals that the academic suspects might be cheating in a timely fashion.

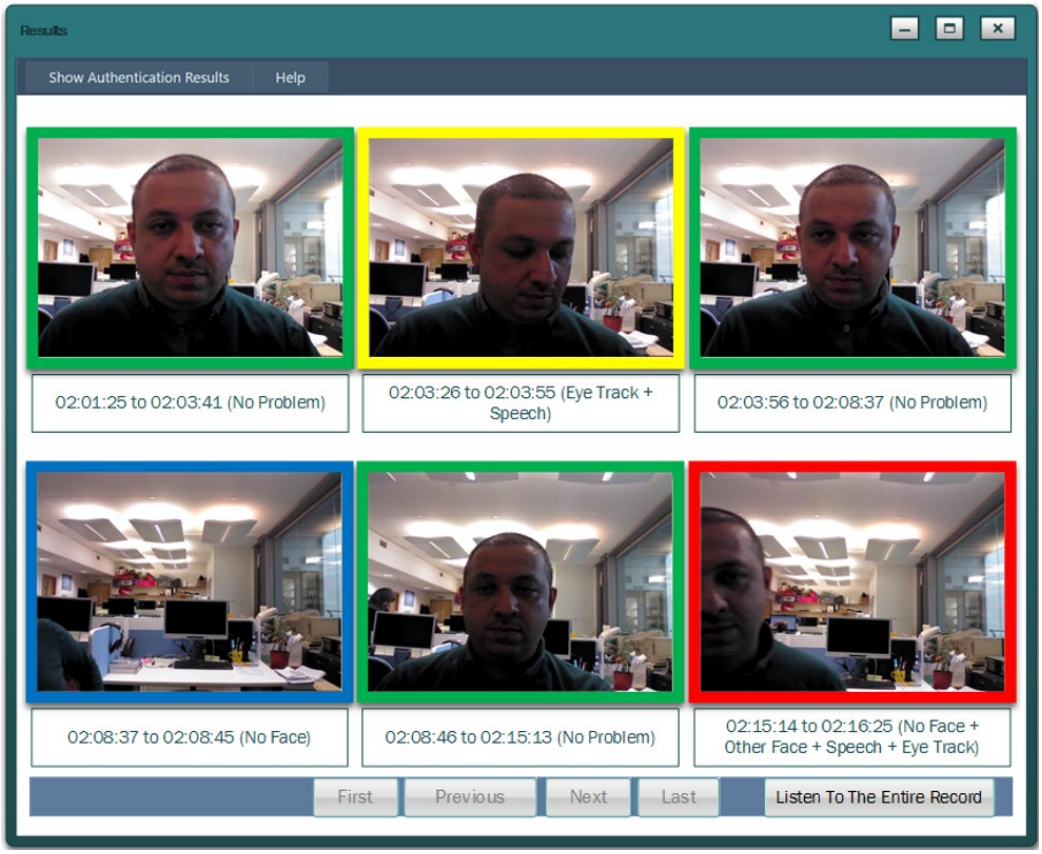


Figure 5.9: The Authentication and Security Results

In Figure 5.9, for techniques, such as face recognition, speech recognition or sound recording, these samples provide the assessor with a further manual confirmation if required. The green rectangle around the photo means there is no problem in both biometrics and security test, the yellow rectangle indicates that there is a security problem during this period, such as eye tracking, head movements or speech; the blue rectangle refers to an identity verification problem occurred, for instance: no face or even another face in front of the camera, and

samples marked in red are those that have failed in both biometric identity verification and security test. The academic can also navigate to show more results, and if required, listen to the entire recorded sounds during the exam time.

To show all the captured photos of a specific security or authentication problem among those recognised misuses, the academic can click on the same photo then the system will present further more inner interface summarises/organises the taken photos during this particular time/misuse period as depicted in Figure 5.10.

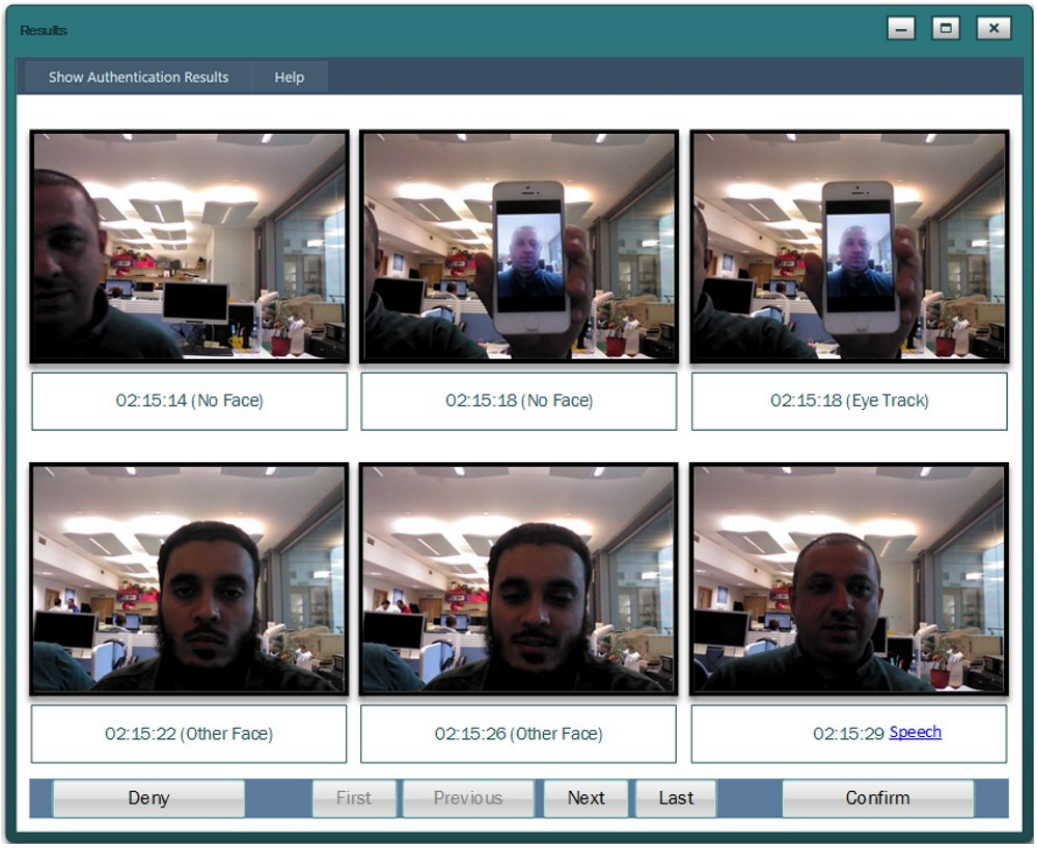


Figure 5.10: Detailed Authentication and Security Results

Utilising this interface, the academic can see the required details that help him/her to deny or confirm cheating (by clicking the buttons shown in Figure 5.10). The academic can also navigate to show more results or even listen to the short recorded talks that have been recorded during the test that indicates potential cheating, they are these duration of sounds that have been clipped from the entire session recording, which are basically recognised by the speech recognition algorithm. If the academic confirmed someone cheated, then the system will provide a report of that cheating as accessible evidence that might be required in future to prove the electronically dedicated misuse during this online test. Figure 5.11 depicts this final printable report.

Figure 5.11: Final report summarises cheating

Finally, the system could produce a PDF-based report and this effectively is the evidence that can be stored for a long time and used in future alternatively.

5.3.1.2.5 Help

Finally, the Help tab, for both academic and student viewpoints, has the same content with further inner tabs (About and Contact). Furthermore, with the final version of the system, it is planned to provide a demo video showing/simplifying how to use the system effectively.

5.3.2 Student Perspective

Generally, in order to accomplish the e-invigilated e-test, there are seven steps (as illustrated in Figure 5.12) that the student needs to follow including:

- The student needs to go to the University to take the exam on a lab computer (or install the system on his/her personal computer, laptop, or tablets).
- The students log in with their University credential.
- The student should achieve all the required biometric enrolments (if he/she has not enrolled previously).
- The system will show student's exams.
- The student will select the exam to start.
- The invigilation processes will run during the exam time.

- The invigilation (identity verification and security) results will be saved in the server for later processing.

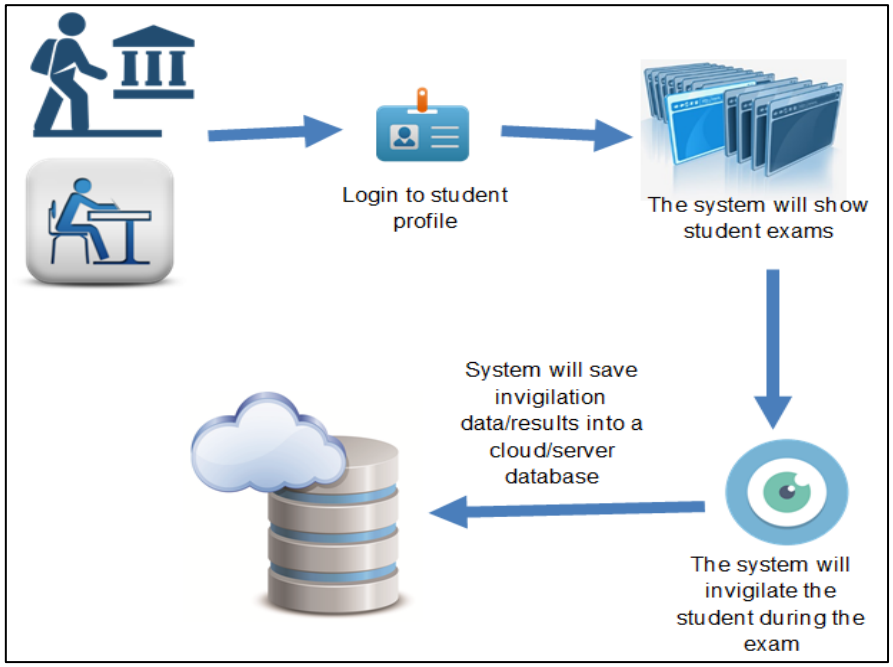


Figure 5.12: Student Subsystem Flow Diagram

The principle of ease of use has been given a high priority in this part of the system; the system provides many simple windows with clear instructions. There is no need for registration process in the students system, all what they need is to enter their domain username and password in the Log In fields then the system will recognise and lead them to an appropriate page that enables them to enrol in the system for storing their templates to be used later on for the identity verification process, view their tests, and taking the online assessments.

5.3.2.1 Student Main Tabs

After entering his/her username and password, as shown in Figure 5.2, each student will be recognised according to the information in the directory entry and redirected to the general home page. Once the student logged in, the system will show four tabs to be used by the student (Figure 5.13). The first tab from the left side of the menu bar is the system general rules (some guiding information), the next is a tab provides the ability to achieve the required biometric Enrolment (or Re-Enrolment), then *MyTests* tab (to show student's available tests), and the last one for help, in addition to the logout link to provide the ability to log the student out.

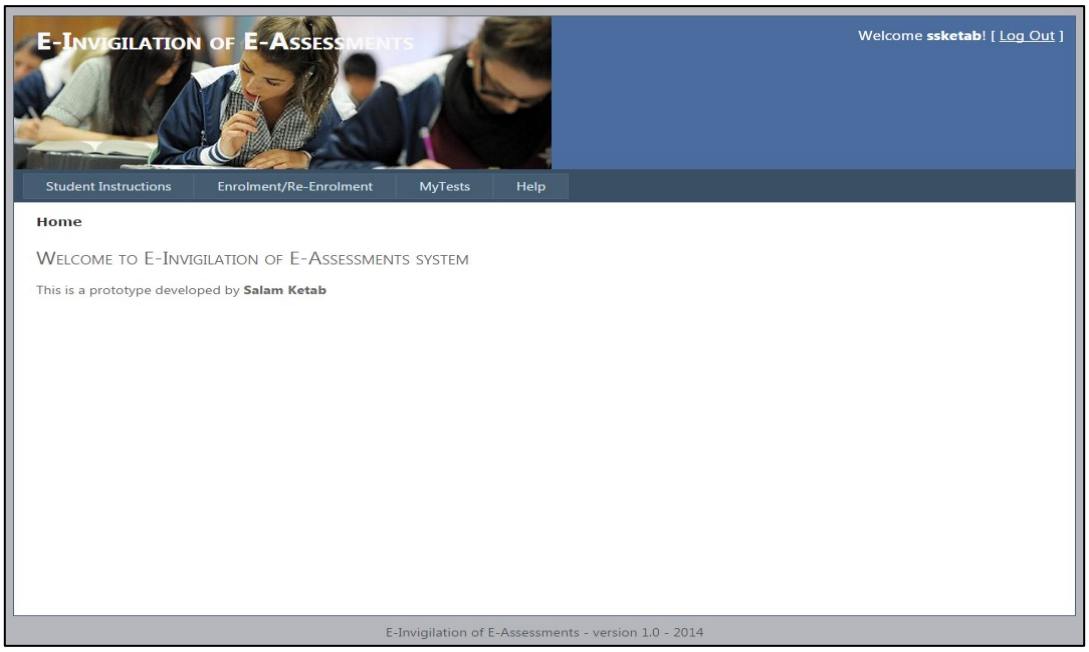


Figure 5.13: Student Subsystem Main Tabs

5.3.2.1.1 Student Instructions

Even it is a simplified and clear website, as depicted in Figure 5.14, there are many instructions that the student should read before utilising it especially if he/she uses the system for the first time, these instructions can be seen by the student in *Student Instructions* tab. Moreover, there are many illustrative messages to describe some unforeseen situations.

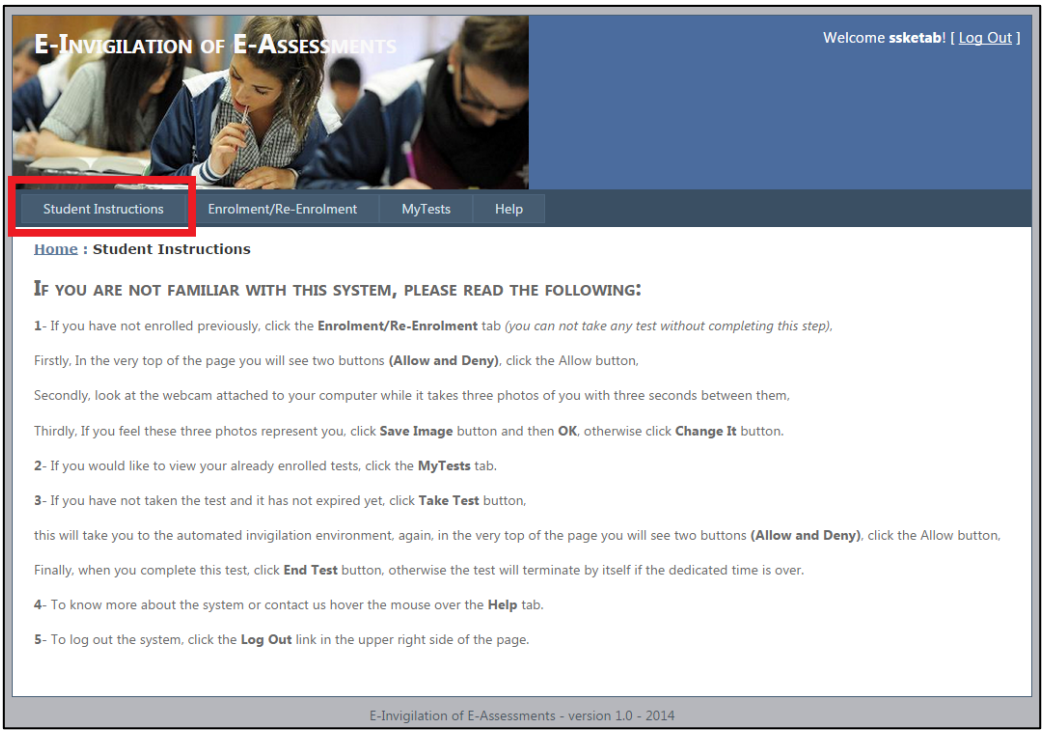
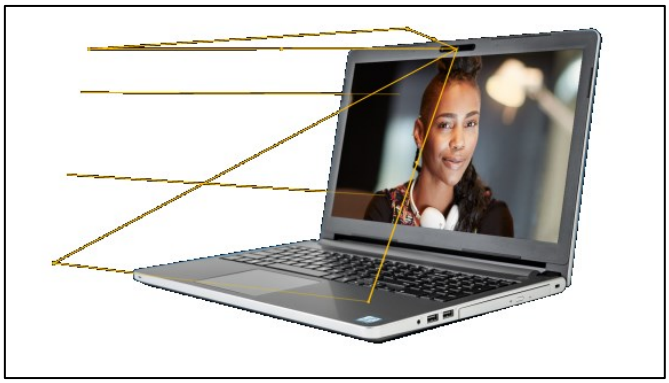


Figure 5.14: Academic Instructions

The system offers facial recognition using a 3D camera to recognise a student's face and to record sounds during the exam via the microphone. Moreover, the system implements eye tracking (using an Eye Tracker) to follow and record the student's eye movement.

- A front-facing Peripheral Creative 3D Camera (F200, Windows Platform): This device helps to recognise student face using conventional camera and records sounds during the exam via microphone array. The infrared parts (infrared laser projector, and infrared camera) allow Intel RealSense to track head movement, multiple face detection, measure distances objects, and offer much better facial recognition than a traditional 2D camera. This camera has also been used for recording sounds during the exam via a built-in microphone. It has SDK that supports C#, C++ and Java that can be used by the windows application. After exploring many kinds of 3D cameras that were available when building this prototype, this camera was the best available one and reasonably priced hardware and software. As shown in Figure 5.15, from March 2015, various laptop and tablet computer of the most well-known computer producers in the world including: (Asus, HP, Dell, Lenovo, and Acer) have started offering one or more devices with Intel RealSense camera built in (Intel, 2016a).



Source: Intel, 2016

Figure 5.15: A Built-In 3D Camera (Intel RealSense Technology)

- Eye tracker (The Eye Tribe): This device helped to track student eye movement (x and y coordination); it is working separately from the 3D camera; and it also has SDK that supports C#, C++, and Java that can be used by the windows application. There are variety of encouraging factors to choose this particular device such as the availability and cost. There are at the time a range of technologies that have been introduced to do eye tracking technology that were the reasonably priced because previous eye tracking hardware and software tended to be very expensive, and Eye

Tribe was the most reasonably priced of them with the leave time for delivery was quicker than the other had. It is not expected that the performance of the other eye tracking software to be less efficient than Eye Tribe, but the objective here was not looking to evaluate different eye tracking products it was just looking to pick one and Eye Tribe had to be the best one. Furthermore, Eye Tribe was also chosen because it came with an easily used SDK whereas the other devices tend to be just simply for plug and play into game applications with lack the ability to interact with them.

5.3.2.1.2 **Enrolment/Re-Enrolment**

If the student has not enrolled previously, he/she should click the Enrolment/Re-Enrolment tab to complete all the required biometric enrolments (completing the required biometric enrolments is mandatory). The enrolment page will appear in front of him/her, for privacy purpose, in order to take the photos, the student will be asked to allow the camera to turn on. Then, as illustrated in Figure 5.16, to complete the enrolment or re-enrolment process he/she should look at the webcam attached to his/her computer while it takes the photos. The candidate then has the opportunity to decide whether the taken photos are representative of them or not. In this process, only a legitimate user should be involved, so the academic needs to perform a check using the university enrolment data.

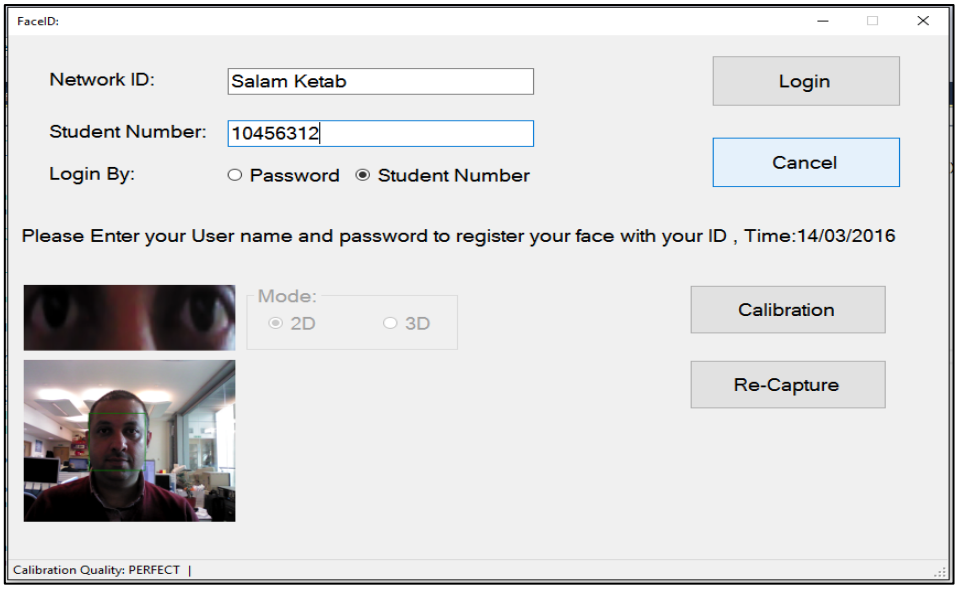


Figure 5.16: Face Recognition Enrolment/Re-Enrolment Process

The student can calibrate the basic eye movement around the screen as shown in Figure 5.17. For details about complete initial eye tracker calibration, re-calibration and installation operations please see electronic Appendix F.

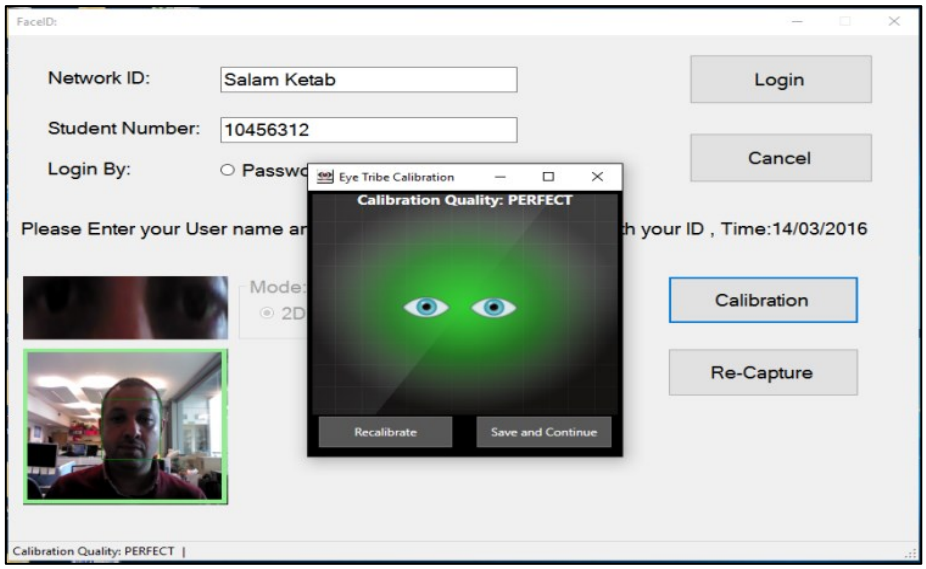


Figure 5.17: Eyes Calibration

5.3.2.1.3 MyTest

If students would like to view their tests, the system can supply them with a list of taken, expired, future, and available tests. On the right side of each test there is a (Take Test) button that can be clicked by student to take that assessment if it is available, otherwise (e.g. the test is taken, expired, or will be available in future) an appropriate message will appear to that student telling him/her details about such assessment. Figure 5.18 shows the list of taken, expired, in future, and available tests (table of the student's tests).

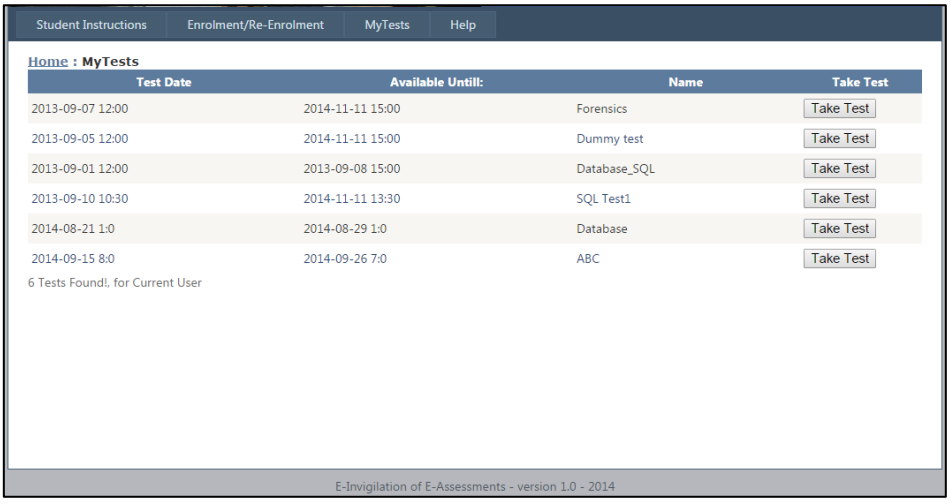


Figure 5.18: A List of Taken, Expired, in Future, and Available Tests

After clicking the Take Test button, if the test is available, the system will direct the participant to an automated and controlled invigilation environment.

With the biometric requirements in mind (in particular universality, collectability and acceptability discussed in 3.2.3), when it comes to implement the proposed architecture in Chapter 4, a number of practical decisions had to be made such as which biometric modalities and security technologies to be utilised in order to provide continuous identity verification and system level security given what is practically available. Thus, there are lots of things to have done and it about managing the time and making sure that the basic core framework and the system was developed to get to test the research hypothesis rather than developing a fully working system. Therefore, when it came to biometric modality, the selection was limited due the many factors including the priority, cost, and some modalities just about available. Therefore, there is a big disparity between what theory says and what the available biometric technologies that could be achieved in reality, however, of those face and finger are by far the easiest and most mature technologies. Yet, due to the lack of transparency, the finger is not suitable to be utilised in the proposed architecture. Therefore, the research decided to focus upon the use of facial recognition as the underpinning continuous and transparent biometric modality. As face technology represents one of the easiest and most widely available biometric modalities and it is most mature. Generally, additional work needs to be done with some other modalities (e.g. iris recognition, head or eye movements) to aid them, and other might be weak and not available commercially (e.g. mouse movements). Moreover, essentially the nature of the activity that the system is going to do was not typing or voice based which negated the need for other biometrics such as keystroke analysis or voice recognition. Therefore, the selection of biometric modalities is largely upon what the system is trying to get them to do.

This study has explored the use of facial recognition in both 2D and 3D modes employing the latest technology (Intel RealSense with 3D camera) that has been decided to play around with the performance and investigating the impact that 2D vs 3D facial recognition is going to have. But unfortunately, at the time of building this prototype, there is no available technology that could provide 3D facial recognition in the entire market. Therefore, after some correspondence with the Intel RealSense technology manufacturer, in addition to the available 2D facial recognition, the best what the Intel SDK can offer and the easiest what could be done is to provide 2D plus depth information (utilising the ability of the 3D camera that provides depth information in the 3D mode) in order to achieve a better performance by developing an enhanced version of 2D facial recognition. The result is a semi 3D technology, and from now onward the research will refer to it as 3D facial recognition simply because the

actual algorithm was not available but it is not a huge stretch in the imagination to think that in time that would be replaced by a complete 3D facial recognition system. Therefore, the underlined recognition system is the same for 2D and the 3D but the 3D introduces further information about depth perception (yaw, pitch, and roll) and that is a binary decision that leads them to the decision box. An investigation of using Iris has also been done, but actually the system struggled to get the quality of the signals (with the available eyes photos) and the researcher realised it would soon become a whole new body of work developing a partial iris recognition system to work and begin to fill that scope and area away from the research objectives, as essentially it was not the purpose of the research to develop biometric modality techniques themselves. Therefore, what it has been accomplished here is very much a product of what it could be achieved within the time frame with what is available.

Therefore, the system will offer continuous identity verification using a front-facing 2D/3D camera:

- 2D facial recognition: It is the main (user-friendly) authentication approach that has already been used in the prototype e-invigilation system (Ketab et al., 2015). However, this method could be bypassed by spoofing facial recognition using a photograph.
- 3D facial recognition: for more robust facial recognition, this phase of the work has focused upon the development and evaluation of novel continuous and transparent authentication utilising depth information (distance and head movement) for adding a further dimension to facial identity verification using a 3D camera. The suggested algorithm utilises the depth information provided by an infrared camera as the main factor to enhance recognition over the 2D method.

The EIEA system offers many layers of security including:

- System Log In: In order to log in the system, the users will provide their username and student number and/or password.
- 2D and 3D facial recognition (verification).
- Continuous Eye Tracking: Using the eye tracking technology (the Eye Tribe) to follow and record the participants' eye movements or locations (x,y) to check whether they were focusing on the computer screen. The eye tracking is linked to the camera

to take a picture whenever the student moves his/her eyes away from the screen for a period of time.

- Continuous Head Movements Tracking: Utilising the 3D camera, the system can continuously recognise, capture and record all times and durations of participants' head movements (turn right, turn left, up, and down) to check whether they were focusing on the computer screen.
- Speech recognition* and recording: in addition to capturing/recording the whole session, the 3D camera also has a built-in microphone with noise-cancelation ability to get a clear voice recording to record the sounds during the exam time (continuously).

  For privacy, avoiding/filtering unnecessary sounds recording, and using the available storage effectively, the system has captured the human speech then saved it as texts, and recorded all times and durations of them. This has been achieved utilising the textual representation of grammars for use in speech recognition (Java Speech Grammar Format or JSGF** for short).
- Utilising the 3D camera, the system can continuously recognise, capture and record all times and durations of any other or different face(s), more than one face, or even no face at all (providing multiple face detection).

After enrolment, when a participant logs in the system to take the online assessment, all the authentication and security monitoring approaches will operate simultaneously to check the authenticity and detect any cheating. For the continuous identity verification, each captured sample will be named and stored in the system database every 4 seconds. There is a need to capture regular samples but not on such a regular basis as to inhibit the operation of the system in terms of requiring too much processing, storage, and communication, therefore, for the purpose of this prototype it has been decided to be every 4 seconds to provide sufficient samples to do this. At this exact time a matching process occurs with the stored template in the Intel RealSense database, the decision then will be made relying on the Intel RealSense classification algorithm. The same process will be accomplished in the 3D mode in addition to the role of the depth information to enhance the authentication process. A screenshot has been taken to illustrate the complete group of real time or actual system numeric and logical parameters in Figure 5.19.

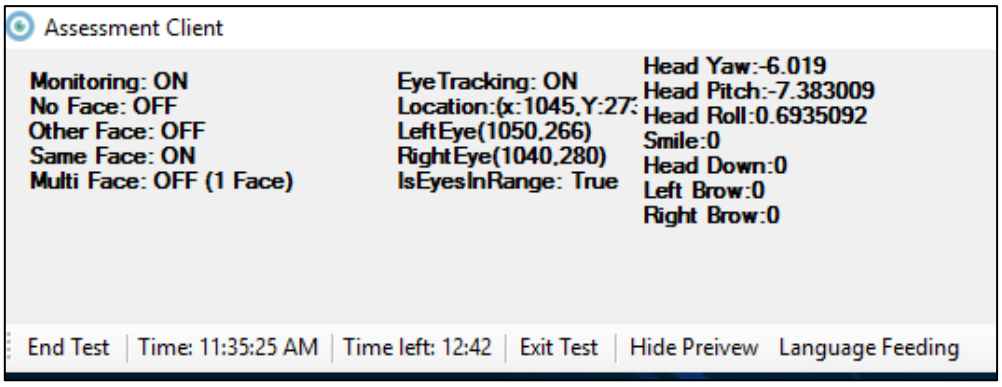


Figure 5.19: System Real-Time Parameters (3D Mode)

These parameters provide real time Boolean and numerical information for debugging/testing purposes; however, in reality, the student would need some of them. They show:

- continuous monitoring statuses (in case of no, other, same, and multiple faces),
- continuous eye tracking (location, left eye, right eye, and is-eye-in-range),
- continuous head movements (yaw, pitch, and roll), and
- face expressions (including smile, head down, and eyebrow movement).

The above parameters indicate:

- Monitoring: either ON or OFF, which means the 3D camera is being monitoring the participant without problems or participant's face absence (the system could put limits on how much the monitoring process can be OFF, for example, if the student left the position for N minutes then the system will turn the test off rather that continuously recording misuse that would store unnecessary data on the disk).
- No Face: either ON or OFF, which indicates there is a face in front of the camera during the exam time or not.
- Other Face: either ON or OFF, which indicates if there is another face(s) other than the legitimate participant in front of the camera during the exam time or not.
- Same Face: either ON or OFF, which indicates if the face of the legitimate participant is currently appearing in front of the camera or not.
- Multi Face: either ON or OFF, which indicates there is another face(s) in addition to the legitimate participant in front of the camera during the exam time or not. Furthermore, the exact number of faces in particular time can also be indicated.
- Eye Tracking: either ON or OFF, which means the eye tracker sensor monitors the participant without problems.

- Location*: this gives the centre point (x, y) of the current focus on the computer screen of the participant's eyes, which is calculated relying on both left and right eyes positions on the screen at the same time.
- Left Eye (leftEye) & Right Eye (RightEye)*: this gives the exact locations (x, y) of the current focus on the computer screen of the participant's left and right eyes.
- Is The Eyes in Range? (IsEyesInRange)*: either True or False, to identify whether the participant's eyes sight within the virtual predefined boundaries by the custom software.
- Head Yaw*: this gives the exact current location of the head yaw which relates to the axis that a person shakes their head on continuously.
- Head Pitch*: this gives the exact current location of the head pitch which is when the head nods continuously.
- Head Roll*: this gives the exact current location of the head roll which is when the head leans to either side continuously.
- Smile*: it gives one of the face expressions identification that can be provided by the 3D camera, this is a number equal or less than 100 which is the percentage of participant's face smile expression.
- Head Down*: it indicates the participant's face position whether it is in a straight positioning or bent down.
- Left/Right Brow*: it gives one of the face expressions identification that can be provided by the 3D camera, this is a number equal or less than 100 which is the percentage of participant's left/right eyebrow location comparing with the original location of the face template in Intel RealSense database (in the biometric enrolment stage).

* Those at star are actually only for testing purposed they are not for to be core to what the student needs to understand in order to interact with the system.

The above buttons indicate:

- End Test: provides the participant the ability to start or end the test at his/her convenience (it is initially Stat Test button).
- Time: this indicates the current time which is fetched from the computer being used during the experiment.

- Time left: it informs the participant the remaining time of the test till the end of the test.
- Exit Test: it gives the participant the ability to quit the entire application in order to return to the computer desktop.
- Hide Preview: this provides the participant the ability to hide/show the above part of the screen in case he/she would like to get more space for the below test area.
- Language Selection: this gives the researcher the ability to change the dictionary (language) or increase/decrease the word count that is being used during the experiment for speech recognition in a particular dictionary.

During an exam that taken by a student, whenever action/issue occurs, the start and end times of that unique issue will be recorded for later authentication and security decisions. All these details will be recorded in a dedicated table called Issues as shown in the following Table 5.2 (Issues).

Issue ID	Issue Type ID	Issue Starts	Issue Ends	Student ID	Test ID
1	5	2016-02-08 09:55:14	2016-02-08 09:55:14	1	1
2	5	2016-02-08 09:55:15	2016-02-08 09:55:20	1	1
3	3	2016-02-08 09:55:16	2016-02-08 09:55:17	1	1
4	2	2016-02-08 09:55:17	2016-02-08 09:55:19	1	1
5	3	2016-02-08 09:55:19	2016-02-08 09:55:20	1	1
6	2	2016-02-08 09:55:20	2016-02-08 09:55:20	1	1
7	4	2016-02-08 09:55:20	2016-02-08 09:55:24	1	1
8	5	2016-02-08 10:02:45	2016-02-08 09:55:25	1	1
9	5	2016-02-08 09:55:37	2016-02-08 09:55:38	1	1
.	.	……...	……	.	.

Table 5.2: Issues Table

Every issue has a unique number under the *Issue ID* column. The *Issue Type ID* value within the *Issues Table* corresponds to the *Issue Type ID* value in the *Issue Type* Table. The exact time of the start and end of each issue will be recorded under *Issue Starts* and *Issue Ends* columns. These periods of times are essential in order to make the accurate security decisions. For instance, if there is no face for a period of time started from 09:55:20 to 09:55:27 which is 7 seconds, and the predefined time limit that allows such issue to occur was only 4 seconds which is less than the captured period (face absence), then the system will consider this as misuse action and a report will be sent to the academic accordingly. They are also these time starts and ends that can be used to calculate the duration of time when

somebody was speaking to take a precise period of recording sound to send to the academic as potential cheating evidence or even to be utilised for voice verification (see Table 5.3). The table also contains the *Student ID* and *Test ID* that correspond to the IDs in the main *Student* and *Test* tables and they are required here to refer to the exact student in the institution and the exact test among the tests that he/she has taken.

After completing the registration and calibration processes, the student then can log in the system at any time he/she would like. It is also this the verification (in addition to using the username and password/student number) for student log in security step, which can be considered as the first step to harden the system against the imposter, for instance, in case if an imposter logs in using another user's credentials. Then the identification algorithm firstly performs the 2D facial recognition and if the user has passed, then it performs the 3D facial recognition and if he/she has passed, then the log in icon will be activated to enable the participant to click it to log in the continuously monitored online assessment environment, otherwise the system will present appropriate message telling that the user is not the legitimate one. These two additional log in face recognition security would help to prevent further types of misuse such as using a full colour photo of a legitimate student to log in.

In terms of the volume of data on the system storage memory, the image samples can be considered the largest data size that might take the majority of the space on the disk. Therefore, taking a wise decision for storing the suitable volume and number of image samples (and other large size data such as the entire session sound recording) will impact directly and positively on the efficiency of the entire system and enhance its performance. An example has been discussed in section 6.4 regarding the data sizes to prove the feasibility of the data storing strategy of the proposed approach.

A screenshot of the main simulated online assessment has been demonstrated in the following Figure 5.20. The figure also shows the other real-time parameters such as monitoring status and eye tracking information.

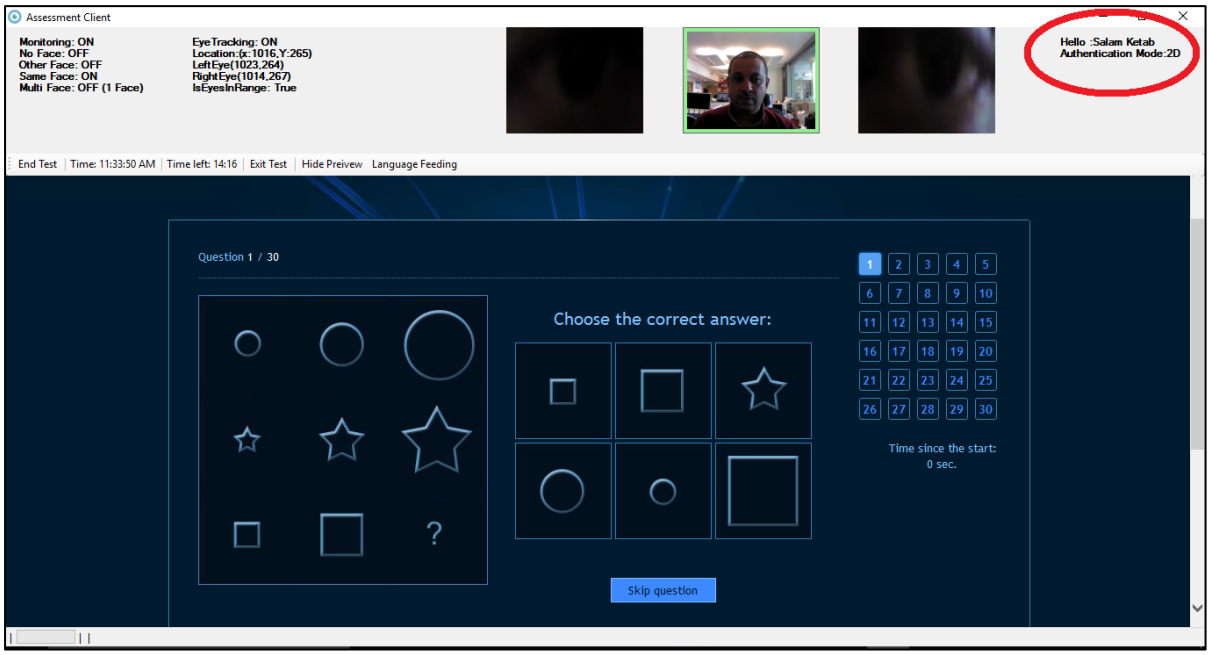


Figure 5.20: The Main Simulated Online Test in the 2D Mode

In addition to the previously explained real-time parameters, Figure 5.20 also displays the real-time video stream of the participant's face and eyes, as well as the 2D/3D facial recognition mode indicator in the upper right side of the screen. A continuous user identification using 2D facial recognition algorithm is continually enabled (every 4 seconds), and their facial features are compared with the information in the 2D facial recognition Intel RealSense database.

During the 3D mode, as illustrated in Figure 5.21, all the Creative 3D camera depth and infrared abilities are utilised including multiple face detecting, continuous head movements recording and face expressions recognition.

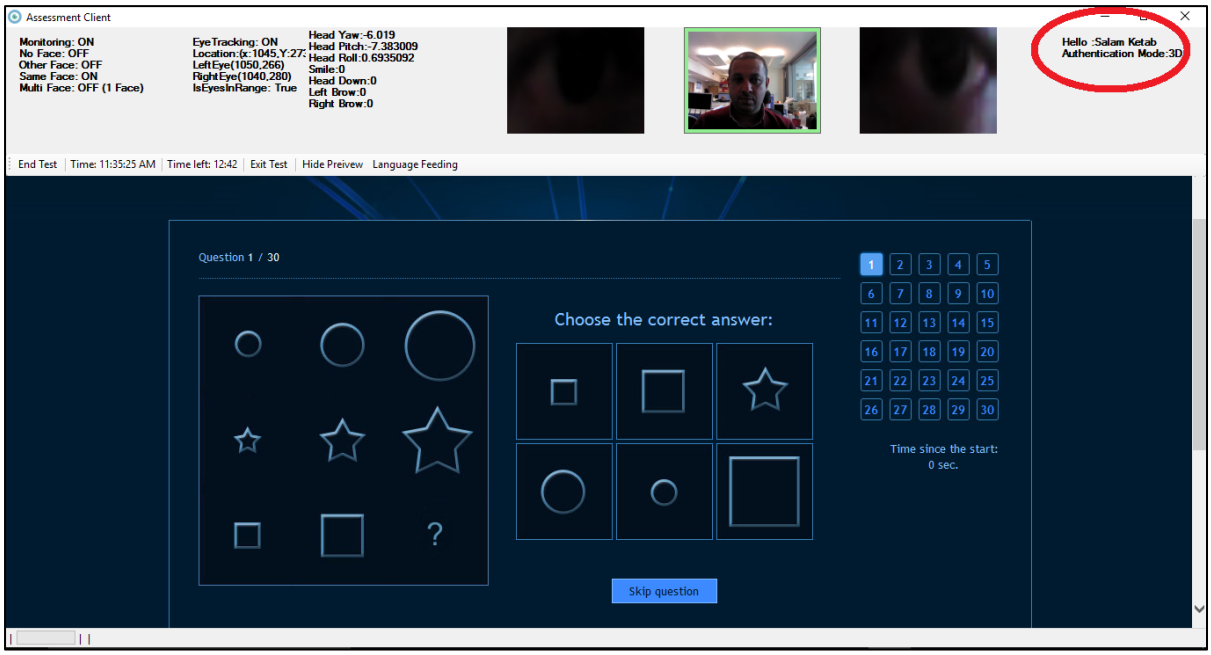


Figure 5.21: The Main Simulated Online Assessment in the 3D Mode

A continuous user identification using 3D facial recognition algorithm is continually enabled (every 4 seconds), and their facial features are compared with the information in the 3D facial recognition Intel RealSense database.

The eye tracking security subsystem will continuously be run during both 2D and 3D modes. The tracking results (the captured photos and all left, right eye movements and the calculated centre locations, in addition to the exact time of each of them), about 30 samples (for each eye to calculate the centre location) every second, will be tracked, calculated then stored (for later analysis that helps to make a decision to send a report indicates cases of misuse or not).

Relying on the eye tracking technique, the developed algorithm has been written to give an order to the Creative 3D camera to take a photo of the scene with every participant's eyes sight is outside the boundaries of the computer screen. However, in order to consider the case as cheating attempt by the participant, the absence of eye sights of the screen boundaries should take N seconds (this period of time, as has been discussed in Chapter 4, can be changed according to the academic desire); in such case a report about this misuse has to be sent to the academic.

All the speech recognition results, times, and durations have been saved in the system database as illustrated in Table 5.3, it is this table that contains every spoken sentence by anyone was speaking during the session relying on the aforementioned algorithm.

Speech ID	Speech Text	Speech Date Time	Issue ID	Speech Duration
1	what is the correct answer	2016-02-08 15:16:33	1	2129
2	only one choice	2016-02-08 15:16:35	2	969
3	the answer is b	2016-02-08 15:16:37	3	933
4	on not in	2016-02-08 15:16:42	4	359
5	of	2016-02-08 15:16:45	5	250
6	were	2016-02-08 15:16:47	6	344
7	the up side of it	2016-02-08 15:16:49	7	1679
8	will	2016-02-08 15:16:49	8	359
9	what do you think the call	2016-02-08 15:16:53	9	2039
.	……..	……	.	……

Table 5.3: The Speech JSGF Table that Contains the Spoken Sentences during the Experiment

For every captured sentence, the table shows speech date and time that can be used to indicate the start of the spoken sentence. The exact period of that the sentence has spent is identified, it is this period that can be used with the start time of the sentence/word to calculate and identify the exact position of the sentence on the recorded session, then it will be clipped to be used as evidence of cheating, the academic can go to specifically the point in the place where those words were spoken to review the facial samples in more usable and systematic fashion. The head movements (Roll, Yaw, and Pitch), in addition to all instant time occurrence of each of them, will be measured and recorded continuously during the 3D mode only. The Intel RealSense technology provides the ability to recognise/detect the face expression including eyebrow down and smile. With every eyebrow down and smile a photo of the participant's face will be taken, named and saved in a dedicated location on the disk for later processes. Those two facial expressions particularly will be captured to explore whether the changes in the participant's face expression have a negative impact on the simultaneous (continuous) facial recognition authentication.

During the exam time, if there is no face (absence or hidden) in front of the screen of the computer, the 3D Creative camera can easily identify this case, then a snapshot of the scene will be taken, named and saved. Furthermore, with predefined angle limits of the participant's face orientation, the creative camera was also taking photos of the participant's face whenever he/she bends his/her head down, turns it left, turns it right or moves it up. This to detect the student's face whenever its orientation different from the predefined angles limits. The 3D Creative camera can easily identify these cases, and a photo of the face will be taken simultaneously, then named and saved to be used as an evidence of potential misuse.

The student's input data has been categorised into groups of actions or captured misuse. The maximum number of these actions in one assessment is 17, depending on the activities that have been achieved by the participant during the exam time. these categories are: all the collected data including 2D and 3D facial recognition samples which will be taken every 4 seconds (*2D FR Samples and 3D FR Samples*); the entire session recorded sounds (*Audio Recording*); the failure matching results of the 2D and 3D facial recognition modes (*Different Face 2D and Different Face 3D*); the images that will be taken in the case of participant's face expression changing i.e. eyebrow down or smile (*Eyebrow Down and Smile*); the images that will be taken for the record of eye tracking including the file for all the coordinates of the eye movements, more than one face, and the absence of any face issues (*Eye Tracking, More Faces, and No Face Images*); the successful matching results of the 2D and 3D facial recognition modes (*Same Face 2D and Same Face 3D*); the file for all the coordinates of the head movements (*Head Movements*); and the images that have been taken for the record of turning the face down, left, right and up (*Turn Down, Turn Left, Turn Right, and Turn Up*). However, not all types of actions exist in every test; this depends on the activities that will be done by the participant and the impact of surrounding environment during the test time, which is why the number of actions varies from test to test.

* *"Speech recognition systems provide computers with the ability to listen to user speech and determine what is said. Current technology does not yet support unconstrained speech recognition: the ability to listen to any speech in any context and transcribe it accurately. To achieve reasonable recognition accuracy and response time, current speech recognizers constrain what they listen for by using grammars"* (Oracle, 2016).

** *"The Java Speech Grammar Format (JSGF) is a platform-independent, vendor-independent textual representation of grammars for use in speech recognition. Grammars are used by speech recognizers to determine what the recognizer should listen for, and so describe the utterances a user may say. JSGF adopts the style and conventions of the JavaTM Programming Language in addition to use of traditional grammar notations"* (JSGFGrammar, 2016).

5.4 Conclusion

There is no doubt that there are many difficulties can be faced during developing such system; starting from the design of the database which will contain/manage the necessary system data, through determining the essential system requirements that bring further barriers that must be tackled in order to complete designing an efficiently working system, to the last but not least taking in account the end user convenience. In the design of the interfaces, the principle of ease of use was given a high priority. Furthermore, it was essential to develop a system capable of providing the academics with a prioritised and usable interface to verify and check cases of possible cheating.

The system was developed to get to test the research hypothesis rather than developing a fully working system. In order to balance between the principles of transparency and robustness of the chosen modalities, the face recognition in 2D and 3D modes was the easiest, most mature, and appropriate technology to be employed. It was significant limitation on the ability to involve many other modalities, as it was just a challenge to find appropriate recognition system to implement because currently they are not exist, expensive, and do not meet the principle of continuous and transparent authentication. However, the purpose of the study was to look at a continuous identity verification, the security of the system, and of the nature of the interfaces that result in order for academic to identify cheating in a more reliable mode, thereby the purpose of the PhD was not solely to provide different forms of biometrics.

6 EIEA Validation

6.1 Introduction

This chapter presents the validation of the developed system to provide secure, flexible, transparent and continuous identity verification and security monitoring to identify cheating in e-assessments. Given the requirements that have been identified in Chapter 4, the core research questions to be addressed are:

- Can the system reliably capture, process, and identify users through the use of biometrics in a transparent and continuous manner?
- Can the system reliably identify cases of misuse?
- Can the system scale appropriately to manage large volumes of learners?

The answers to these questions will help to prove the applicability and feasibility of the previously proposed e-invigilation of e-assessment system architecture and prototype (Chapters 4 and 5).

Therefore, an experiment (Experiment 1) has been conducted utilising the developed prototype in previous chapter involving 51 participants. Furthermore, in order to evaluate the robustness of the approach against targeted misuse 3 participants were tasked with a series of scenarios that map to typical misuses, such as pretending to be the genuine exam taker (Experiment 2). At the beginning of Experiment 2, each of those 3 participants has also been asked to log in the exam as an intruder by implementing predefined log in thread scenarios, the results of both experiments have proven the expected robustness and transparent of the proposed approach. Therefore, these experiments are looking to explore the reliability of the suggested participant continuous identity verification process, for example, what is the facial recognition performance under normal use, does the participant's facial expressions play a role in the recognition performance (e.g. smile or eyebrow down), and other factors that might affect the performance, such as wearing glasses or head veil during the experiment test time. Furthermore, they are looking to examine the transparent nature of the capturing mechanism and how well the system can do this, and the reliability of the biometric sampling. Moreover, under certain circumstances, motivated individuals might want to abuse the system by providing biometric samples, therefore, under those circumstances, Experiment 2 explores whether the system is robust enough to prevent that form of cheating (i.e. to what

degree (the possibility) that someone can forge the participant biometric modality). The sections that follow present and discuss the entire experimental methodologies and results.

6.2 Experimental Methodology

This section presents the scientific methodological approach followed while conducting the main two experiments. An inductive methodology was selected because the research has specified a core set of research questions that need to be examined in an explorative study using participants in order to get certain results, the research is looking for the ability to prevent cheating and then devised the following two experiments that specifically look at both the ability to capture and understand the legitimate user because they try to capture them transparently and under a series of cheating scenarios.

6.2.1 Methodology of Experiment 1: Transparent & Continuous Biometric Identity Verification

In this experiment, the focus will mainly be upon the usability of the system under normal use (Can users be biometrically identified in a transparent and continuous manner?). Methodologically it is common to have studies that involve less than 20 participants as targeted baseline (Mothukuri, 2012; AL-Smadi et al, 2011). The subjects were recruited via e-mail or directly. With the dedicated experiment time in mind, the predominantly targeted were the colleagues (PhD researchers) and staff members in CSCAN; however, the recruiting was also varied among other Plymouth University postgraduate or undergraduate students. The participants just need to be comfortable enough with IT to be able to log in to a web page and complete an online test by answering a series of questions, they are all 18 years old and above agreed and understood all procedure and able to take part in this study.

The experiments were conducted in the Centre for Security, Communications and Network Research (CSCAN) office at Plymouth University on a dedicated computer equipped with the required technologies to accomplish the experiment objectives. Due to the need to the specialist devices in the capturing of the eye tracking and the biometrics, the researcher only had a single computer upon which this would all work, therefore, participants were asked to attend the office to undertake both experiments. The first experiment has been achieved by involving:

- Given Experiment 1 in the above comment, it was necessary to simulate a real test to ensure the experience the participant had would be as real as possible to an e-assessment. As such, participants were asked to take a controlled/monitored online assessment for a maximum duration of 15 minutes as a regular participation. When it came to understand how long the test and how many samples are needed, it is necessary to ensure that the system captures sufficient samples in order to robustly test and understand performance of the operation system, but not to ask the participants to do too much as to make the participant recruitment challenging and difficult to be achieved. And because the system was able to capture samples of different types of data (as explained in details in the previous chapter), therefore, 15 minutes can be considered sufficient period of time, and when looking to other studies in terms of the samples used to justify performance rate, this provides a reasonable baseline of how much to do so. At this stage, the participant will never pretend to be anybody else but themselves. Essentially, there are no bases for understanding false acceptance rate (FAR); as it is basically zero because there was not any threat. Therefore, the participants merely sat down and completed the test and the purpose of that is to see the biometrics and security monitoring of that individual can be used to identify whether there is an issue, thereby only the false rejection rate (FRR) was measured as the research was looking at the usability of the system and its ability to correctly recognise the legitimate user (how will the recognition system work with the legitimate user and not specific imposter).
- Calibration: the participants calibrate the basic eye movement around the screen in order to ensure the right positioning.
- Registration: in this step, patterns of the student's biometrics are collected. For instance, samples of his/her face are captured and stored in the Intel RealSense databases for later 2D and 3D facial recognition.
- Biometric student verification in the log in phase: in each log in, the verification process is done by facial recognition algorithms (2D and 3D facial recognition respectively).
- Participants sat a virtual assessment that contained 30 simple multiple-choice questions. It was ensured that the test questions would take longer than the period required for the capture.

- Continuous participant identity verification via the face recognition algorithms (a sample every 4 seconds), as the camera cannot take concurrently 2D and 3D, therefore, a decision was taken to take 2D facial recognition mode for 5 minutes and 3D facial recognition mode for 10 minutes (the reason why the 3D was 5 minutes longer than the 2D mode because it is new method that required to be explored by spending more time in order to collect more data). The SDK of the 3D Intel RealSense camera comes with the built-in recognition system, the system gives this recognition system a sample then it comes with the decision of one or zero.
- During the experiment, the participants' biometrics/data (2D, 3D, and depth information) and eye movement or focus on the screen will be collected using custom software for that purpose via a 3D web camera and Eye Tracker sensor then saved anonymously in a secure database.
- The security subsystems are continuously running, including:
  - eye tracking (in 2D and 3D modes),
  - head movements (in 3D mode only),
  - speech recognition (in 2D and 3D modes),
  - multiple faces detection (in 2D and 3D modes), and
  - the entire session sounds recording (in 2D and 3D modes).
- Once participants have completed the simulated exam, they will press the Exit Test button (if the 15 minutes have elapsed the test will be terminated automatically) and all information will be held securely within the dedicated computer database. The participants have been provided with the contact e-mail address of the researcher if they would like to be notified of the overall findings from the experimental study.
- All of the information was treated confidentially and data was anonymous during the collection.

Table 6.1 illustrates and summarises the EIEA system configuration settings for the evaluation during the experiment. In general, in this phase of the work, the system algorithms achieve user registration, biometric verification, continuous user identity verification, and continuous security detection.

System Actions	Authentication and Security		
	Log In Verification	Continuous Identity Verification	Continuous Misuse Tracking
2D Facial Recognition	Yes (Once)	5 Minutes	No
3D Facial Recognition	Yes (Once)	10 Minutes	No
Eye Tracking	No	No	15 Minutes
Head Movements	No	No	10 Minutes
Speech Recognition	No	No	15 Minutes
Multiple Faces Detection	No	No	15 Minutes
Session Sounds Recording	No	No	15 Minutes

Table 6.1: EIEA Validation Setting

The complete experiment diagram has been depicted in the following Figure 6.1, that shows the flow of all of the above biometric identity verification and security restrictions.

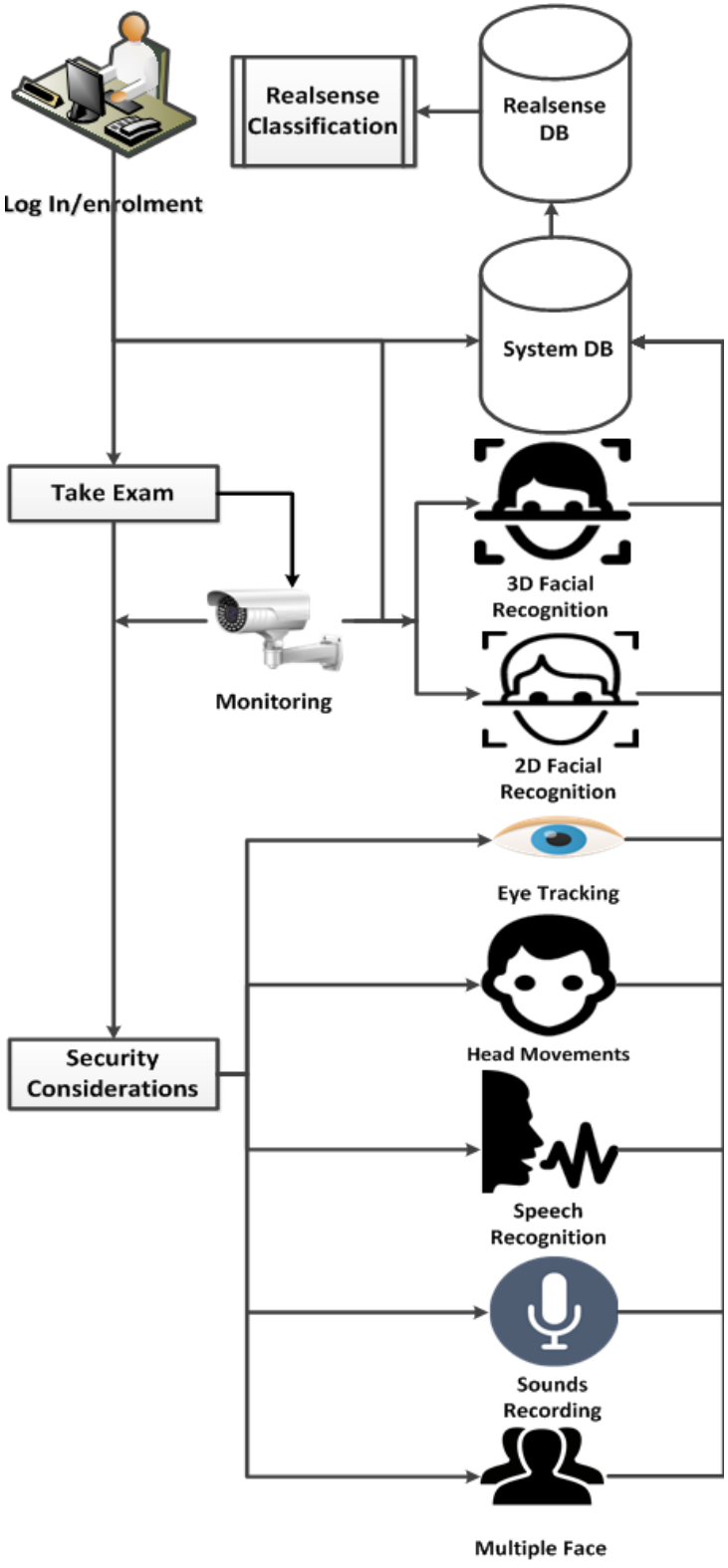


Figure 6.1: Experiment Process Diagram

After enrolment, when a participant logs in the system to take the online assessment, all the authentication and security monitoring approaches will operate simultaneously in order to verify the identity of the participant by matching the collected facial images (in two modes) with the stored templates in the Intel RealSense and detect any cheating attempt.

6.2.2 Methodology of Experiment 2: Targeted Attack

The second experiment focuses upon identifying misuse, a series of targeted attack scenarios are undertaken to measure the effectiveness of the system. In order to evaluate the robustness of the approach against targeted misuse, further to the participants in the previous experiment, other participants were tasked with a series of scenarios that map to typical misuse. Thus, this particular test is not looking to provide FRR but it is looking to evaluate the FAR.

A comprehensive analysis of the literature and the system architecture has come up with a set of threat scenarios that could represent the typical threats both in the log in and during the e-assessment. Therefore, in the beginning of this experiment, each participant has been asked to log in the exam as an intruder by implementing three predefined log in thread scenarios (from 1 to 3), then during the online assessment the rest threats scenarios were implemented:

1. Log in using another participant's credentials. For instance, a student provides another person with his/her username and password to illegally access the e-assessment.
2. Using a full colour photo of a legitimate participant to log in the system. In other words, another illegitimate individual trying to bypass the 2D and 3D facial recognition biometric security.
3. A legitimate participant accompanied with illegitimate participant trying together to log in the system at the same time to pass the 2D and 3D face recognition security barrier.
4. The exam taker leaves the location or the chair (no one in front of the camera) for a period of time.
5. Using the keyboard, mouse, or the laptop mouse pad by somebody else, in which the other person (the impostor) should be very close to the legitimate participant in order to achieve this (two faces in front of the camera).
6. Providing unauthorised help to the participant via answering the questions by another individual orally.
7. Fixing the camera and the eye tracker in front of the genuine exam taker and moving the computer to another illegitimate individual to give unauthorised help (e.g. answering the questions for the rest of the test).
8. Turning the head of the participant to the left, right, up, or down (looking for unauthorised help from somebody else).

9. Using a photo of a legitimate/genuine exam taker in front of the camera by another illegitimate individual (e.g. full colour 2D photo from tablet or smartphone device) trying to bypass the 2D and 3D facial recognition continuous verification of the student.
10. An impostor uses a 2D photograph of the legitimate/genuine exam taker as a mask to bypass the 2D and 3D facial recognition continuous identity verification with eye holes and to bypass the eye tracker security via these holes.
11. Another individual pretending to be a genuine exam taker and sits in front of the camera for a period of time.
12. Asking the participant to wear relatively dark glasses in order to examine the ability of the eye tracker infrared to penetrate the glasses and to explore whether the glasses have any direct impact on the facial recognition performance.
13. Swapping identical twin people, this particular threat can only be achieved by involving, for instance, any two identical twins in the experiment and asking one of them to sit illegally the test that the other twin is taking in order to bypass the facial recognition biometrics.
14. A legitimate participant uses the system resources such as the Internet or flash memory.
15. Sharing the screen, for instance, another individual sits in the opposite side of the legitimate user and share the screen via a kind of connection in order to see the questions (i.e. multi-choice questions) and provide the exam taker unauthorised help through giving the answer (e.g. A, B, C, or D) by sign.

When it comes to implementation, only the first 12 of the above 15 threat scenarios has been chosen as the most reasonable to be tested experimentally to see how the system performs and its ability to identify the misuse, whereas the thirteenth scenario was very difficult to be implemented with the suggested methodology (involving 3 different pairs of identical twins), however, with such threat it is not expected that the current face recognition approaches alone could succeed in differentiate between the identical twin faces. Nevertheless, the theoretical design of the system architecture that has been identified in Chapter 4 would use further reliable biometric modalities (e.g. iris recognition or even scar and mole identification) to help the overall recognition system to take the right ultimate definitive decision. With regard the fourteenth and fifteenth threat scenarios, they are not practical to be implemented as the prototype was not able to achieve these two particular threat scenarios, however, during the

real e-assessment, the theoretical architecture of the system would also normally pick this up through preventing the ability of surfing the Internet, closing the computer ports, using applications other than the examination interface, and the inhibiting capability of screen sharing or any sort of connection with other devices.

6.2.3 Devices Installation

As illustrated in Figure 6.2, the capturing devices have been attached to the computer in front of the participant (the front-facing peripheral F200 3D camera and The Eye Tribe eye tracker). To setup the equipment, please see electronic Appendix F.

Figure 6.2: The Capturing Devices Attached to the Laptop Computer in front of the Participant during the Experiment

Generally, both the camera and the eye tracking software have limitation with respect to the distance that the user away from them, and that was an important consideration in the overall experiment design. Therefore, during the experiment, the participants should sit within this limitation. Taking into consideration the optimum distance of the user's eyes from the computer screen which is between 40 and 76 centimetres (Albin et al., 2008) (this particular distance is suitable to achieve the best performance with both devices), that could help to enhance the participant's convenience and to avoid a high error of the depth measurements, therefore, the participant's face needs to be mostly within this optimum distance. However, the calibration setting (as was described in Chapter 5) itself is setup to make sure the user is

being captured successfully and that itself should force the user to adjust the position accordingly.

It was also important to ensure that the participant was actively involved and engaged within the e-assessment system, however there is no actual need to give them a real test because these are mixture participants from a range of different backgrounds, but in order to make sure both the biometrics and the system monitoring were actually monitoring things as in real environment rather than simply giving them, for instance, a web page or nothing and they might be distracted or might look elsewhere, therefore, it has been decided to give them online IQ test (as shown on the laptop screen in Figure 6.2) to keep them engaged and help to make sure that the monitoring process was actually capturing in a way as it is expected they to do during the real online assessment.

The participants have been given the consent form at the beginning of the study (before the participation in the experiment), should they wish to carry out the study, ensuring their understand that they can withdraw from the experiment at any time up until the end of their participation. For more details in this regard please see Appendix A for ethical approval notifications.

6.3 Experimental Results

The results can be divided into:

- Results of Experiment 1: Transparent & Continuous Biometric Identity Verification.
- Results of Experiment 2: Targeted Attack.

6.3.1 Experiment 1: Transparent & Continuous Biometric Identity Verification

As discussed in the previous chapter, a hierarchal storing strategy has been used to save the collected data such as all image templates and samples, biometric recognition decision results, all surrounding sounds recording. In addition to files to save the head and eye movements data and some tables in the main database to save essential parameters such as paths, dates, times and timestamps. Furthermore, Intel RealSense databases are used to save the 2D and 3D facial image template to be compared/matched continuously with the real time taken samples in both 2D and 3D modes.

The data has been categorised into groups of actions or captured misuse. In order to summarise all the collected samples and actions during the Experiment 1, the following Figure 6.3 is dedicated (The distribution/appearance of those samples and actions in the entire experiment). However, the number of actions varied from test to test.

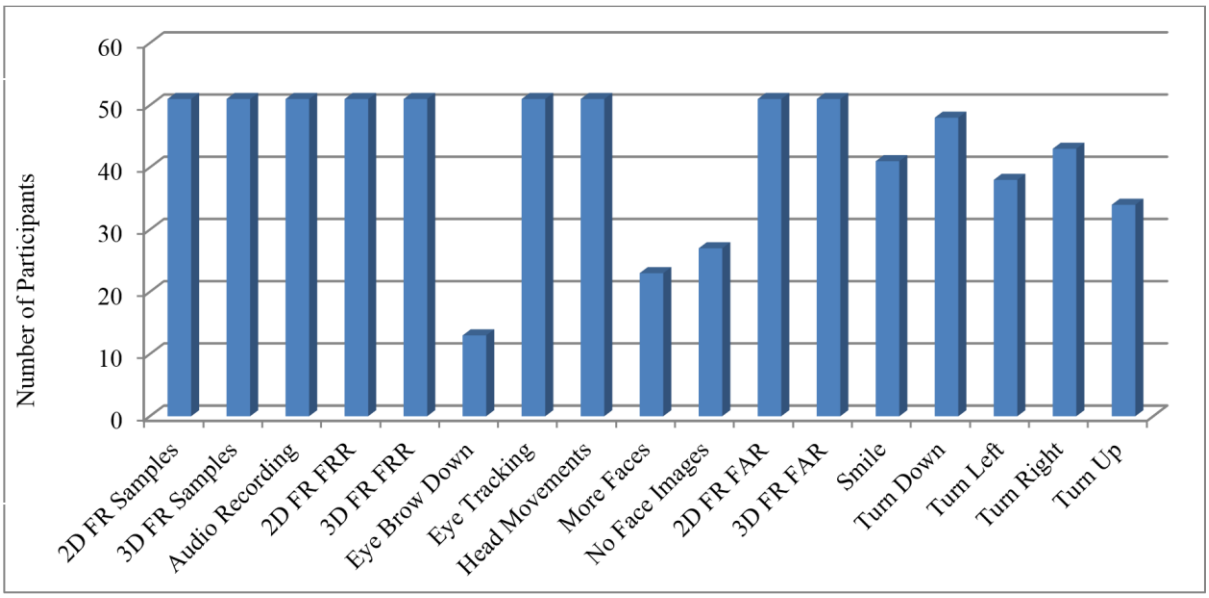


Figure 6.3: The Actions and Samples during the Entire Experiment

Some actions (such as *2D FR Samples* or *3D FR Samples*) were common in every assessment; however, other actions (such as *More Face* or *No Face Images*) occurred only in specific assessments. It is obvious that the expressions were the least actions that happened during the Experiment 1, whereas only 13 tests contain *Eyebrow Down*, less than half recorded more than one face, and about half of them recorded *No Face Images*. Furthermore, a shortage recorded in *Smile* and the *Head Movement* actions. As it will be explained in detail in the following paragraphs, this variation of the actions does not affect the continuous identity verification accuracy for any participant in the experiment (in both 2D and 3D facial recognition modes).

Only the false rejection rate (FRR) was measured as the research was looking at the usability of the system and its ability to correctly recognise the legitimate user. For example, if the system flags up lots of FRR, then potentially the academics being left with reviewing lots of people that were perfectly legitimate and that means the system is not working sufficiently, therefore, the purpose of Experiment 1 was to identify how many did the biometric system picks up and then Experiment 2 was dedicated to looking at specific threat scenarios where there will be people personating in order to identify, in this particular case, the FAR.

Due to the fact that the system was collecting different types of samples during every session of the experiment, the following Table 6.2 has been created to illustrate in detail the distribution and categorisation of all the taken 2D/3D facial samples and reflecting most of the presented actions in the entire experiment of previous Figure 6.3 in addition to the 2D and 3D facial recognition FRR per participant.

This study sorted to collect the number of participants collected by other studies (less than 20) and managed during the period of the collection to collect 51 participants. To achieve the anonymity principle, sequential numbers have been used to name each participant instead of giving the explicit name of the participant. And due to this anonymity policy, the data/images of the participant number 50 is the only data that can be disclosed and explored for experimental validation illustration, as the participant 50 is the researcher himself.

Participant No.	Facial Samples		Actions									FRR per Participant	
	2D FR Samples	3D FR Samples	Eyebrow Down	Eye Tracking	More Faces	No Face Images	Smile	Turn Down	Turn Left	Turn Right	Turn Up	2D FR	3D FR
1	74	149	N	165	1	2	7	8	4	5	4	0	0
2	73	148	N	265	N	1	10	8	15	5	28	0	0
3	73	145	N	179	N	2	3	27	10	40	5	0	0
4	72	145	2	253	3	1	2	3	4	2	3	0	0.096
5	74	149	3	185	4	1	3	3	2	3	4	0	0
6	73	147	N	148	2	N	5	5	14	7	31	0	0
7	73	146	N	241	N	5	25	40	1	4	1	0	0
8	73	149	1	242	1	N	1	43	2	1	N	0	0
9	73	143	N	185	12	4	5	71	52	5	2	0	0.076
10	73	148	5	224	6	N	4	22	N	14	N	0	0
11	71	144	N	169	N	7	42	17	6	2	18	0	0.055
12	73	148	N	65	N	1	4	9	N	2	3	0	0
13	73	147	N	173	N	N	48	28	6	N	N	0	0
14	73	149	N	29	1	1	N	15	14	3	2	0	0
15	72	150	N	35	7	1	N	N	42	N	N	0	0
16	73	150	N	36	N	N	32	30	N	11	N	0	0
17	73	149	11	62	2	4	11	57	19	21	6	0	0
18	73	147	N	192	N	N	1	26	17	12	20	0	0
19	73	149	N	126	N	2	N	39	2	3	N	0	0.006
20	73	148	N	284	N	N	8	37	1	1	N	0	0
21	**73**	**144**	1	257	N	6	**117**	**44**	20	22	2	**0**	**0**
22	71	144	N	372	N	1	N	22	1	15	N	0	0
23	73	148	N	169	N	N	13	60	N	13	N	0	0

Participant No.	Facial Samples		Actions									FRR per Participant	
	2D FR Samples	3D FR Samples	Eyebrow Down	Eye Tracking	More Faces	No Face Images	Smile	Turn Down	Turn Left	Turn Right	Turn Up	2D FR	3D FR
24	74	148	N	113	2	1	5	60	5	41	1	0	0
25	73	148	N	193	N	N	N	30	N	21	N	0	0
26	73	148	N	110	1	N	5	38	N	5	N	0	0
27	73	146	N	280	N	N	5	**100**	**8**	**18**	**1**	0	0
28	74	149	N	35	1	N	2	25	32	N	3	0	0
29	73	145	N	320	N	N	7	48	N	N	N	0	0
30	73	148	N	266	2	N	7	67	1	5	3	0	0
31	**72**	**145**	**78**	232	N	N	22	78	60	1	1	**0**	**0**
32	**73**	**148**	**221**	250	2	N	N	98	N	N	2	**0**	**0**
33	**73**	**146**	10	194	6	N	36	**54**	**56**	**4**	**44**	**0**	**0**
34	73	147	N	280	N	1	4	24	N	5	67	0	0
35	73	147	N	161	3	1	5	119	3	56	N	0	0
36	**74**	**142**	2	**406**	2	N	60	54	6	12	1	**0**	**0**
37	72	148	N	251	1	N	N	N	N	N	2	0	0
38	73	147	N	276	N	N	5	110	2	14	N	0	0
39	73	149	N	65	2	N	N	46	106	N	N	0	6
40	73	147	N	85	1	N	4	37	1	43	1	0	0
41	72	145	N	338	N	N	9	69	19	37	1	0	0.034
42	73	143	5	350	N	N	3	22	1	27	1	0	0
43	72	148	1	148	1	N	31	38	N	4	N	0	0
44	73	147	N	262	N	1	1	10	4	8	2	0	0
45	73	147	N	201	N	N	12	55	110	11	13	0	0
46	72	148	N	202	N	N	3	3	N	1	3	0	0
47	73	141	N	240	1	1	15	7	8	15	2	0	0.014
48	**72**	**147**	N	186	N	N	**95**	**60**	23	9	N	**0**	**0**
49	73	148	N	124	N	N	39	65	1	14	1	0	0
50	73	148	2	190	4	3	2	2	2	2	3	0	0
51	**74**	**148**	5	120	N	3	N	**79**	**4**	**9**	**9**	**0**	**0**
Total	**3717**	**7494**	**347**	**9934**	**68**	**50**	**718**	**2012**	**684**	**553**	**290**	**0**	**47**

Where N means not exist

Table 6.2: The Exact Number of Samples in Every Action and the FRR per Participant

Table 6.2 presents that the samples taken during the eye tracking process recorded the largest number (9934), this due to the fact that the system was very sensitive and taking a photo whenever eye was blinking or eyesight was out the predefined boundaries (computer screen coordination), however this level of sensitivity can be reduced according to the academic desire. It was expected that the samples of the 3D mode (one sample every 4 seconds) to be

one of the biggest numbers, with the average of 146 the total number has reached 7494 samples. Furthermore, in average samples were 73 per participant during 5 minutes of the 2D mode, which makes the total number of samples of all participants is 3717. 2012 samples were taken for face turn down expression, which is relatively large number comparing with the other recorded face expressions that scored 718 (Smile), 684 (Turn Left), 553 (Turn Right), 347 (Eyebrow Down) and 290 (Turn Up) samples. During the entire exam, the camera has been recording all the faces in front of the screen (as it is able to recognise multiple faces), thus 68 photos were taken indicating more than one face were facing the camera at a particular time, these other people's faces appeared in front of the camera because these controlled tests were basically conducted in one of the university labs and there were many other students working around, therefore it just happened to capture some of other faces from time to time. However, these captures have not affected the ability of the approach to efficiently recognise the legitimate participant. Finally, the complete absence of the participant's face (*No Face Images*), as expected, has recorded the smallest number of samples (50).

FRR is the probability that the system fails to detect a match between the input pattern and a matching template in the database, as it measures the percent of valid inputs that are incorrectly rejected. From the 2D and 3D samples that demonstrated in the previous Table 6.2, the FRR results are summarised in the following Table 6.3.

Mode	The FRR of The 51 Regular Legitimate Participants		
	Best	Worst	Average
2D Facial Recognition Results	0	0	0
3D Facial Recognition Results	0	0.096	0.048

Table 6.3: FRR Results of the 51 Legitimate Participants

The FRR was 0 for every participant in the 2D mode and also 0 for 45 of them and less than 0.096 for the rest 6 in the 3D mode, consequently, for all the 51 participants participated in this experiment, the FRR was 0 in 2D facial recognition mode for the best, worst and average results. While in 3D facial recognition mode, the best FRR result was 0, and the worst was 0.096, and hence, the average was 0.048, as some consequent participants' results contain 1 to 14 of 146 rejected samples, this since more probably that the participant's face, at that point in time, was not stable that made the recognition system struggled, for instance, the

participant number 41 all the 5 samples were taken in the same window of time concurrently straight after each other because the user had his head out of shot.

Form the above FRR results, the biometric recognition performance was very good. The nature of the methodology meant the quality of the samples will likely to be consistent (i.e. in same room, same illumination, and typically same physical distance within acceptable parameters), therefore, face recognition algorithms have proven to work very well when given a steady front facial image, and consequently the experiment has proven that the image capturing was very easy, and hence the recognition system performed properly well in the classification of that. However, if this system were deployed on more varied bases, for instance, on some kind of mobile base platform, or at home where it could be dark or the lights off, then the quality and nature of the samples might be different. Therefore, care will still need to be taken in poorer illuminated rooms or environments where the camera position such as where the quality or the angle of the capture may prove problematic. However, the nature of the eye tracking is to ensure that the eyes are in the view of the screen which is exactly where the face recognition camera needs them to be in order to get both of the eyes, thus the orientation is essentially fixed automatically as a product of the design of the system. Additionally, the system fundamentally needs appropriate illumination in order to allow the user to access the test, thus these should help to ensure providing the required level of illumination during the rest of the test. Furthermore, illumination issue will be mitigated with the complete architecture when involving for instance advanced 3D facial recognition (in future) or iris recognition technologies that rely on infrared beams scanning more than face images and even in a completely dark room.

From Table 6.2, it has been proven that the continuous identity verification processes (every 4 seconds) have not been affected by facial expression changes. On average, 78 expressions were identified per user with a total of 3996 samples, nevertheless, there is no direct correlation between the presence of such expressions and the ability of the facial recognition system to do this result. For instance, the participant number 21 who has the largest number of smile expression (117 samples), this large number, however, does not affect the authentication for that particular participant (or other participants who also have a large number of smile expression). The same thing can be said with the eyebrow down expression, where the most obvious cases are participants number 32 and 33 who have 221 and 78 photos of that expression respectively, both participants have perfect authentication results with zero

in 2D and 3D FR FRR. Furthermore, the face angle changes also have not any impact on the authentication (unless it has been considered no face in front of the camera), for instance, many cases including but not limited to participants number 27 and 51, both got excellent identity verification results. Moreover, 6 of the participants have put glasses during the experiment (test time), their continuous identity verification results however were perfect for all cases, which also prove there is no direct correlation between wearing the glasses and the ability of the facial recognition system to do this result. Furthermore, 3 female participants were wearing head veils during the experiment; nevertheless, the FRRs of facial recognition were also perfect with them.

In general, the previous results have shown that the performance of the FRR in the 2D mode in Experiment 1 (regular participation) was better than the performance of the FRR in the 3D mode, however, to enhance the overall system performance, a flipping strategy between the 2D and 3D facial recognition can be employed, for instance, every 3 seconds the mode flips from 2D to 3D, and thus every 6 seconds the system implements 2D facial recognition.

6.3.2 Experiment 2: Targeted Attack

This particular experiment has been conducted to prove the system ability to identify, track, and monitor users with a view to identifying unauthorised help that could be provided by somebody else during the e-assessment. Therefore, this test is not looking to provide FRR but it is looking to evaluate the FAR. Hence, further to the previous 51 participations involved in Experiment 1, 3 participants were tasked with a series of 12 threats scenarios that map to typical misuse in Experiment 2.

The first, second, and third scenarios have been considered as log in threats scenarios, therefore, the following Table 6.4 summarises the results of these three threats separately.

Log in Threat	Participant 1	Participant 2	Participant 3
1	Authentication Failure	Authentication Failure	Authentication Failure
2	2D and 3D Facial Recognition Failure	2D and 3D Facial Recognition Failure	2D and 3D Facial Recognition Failure
3	Multi Faces Capture	Multi Faces Capture	Multi Faces Capture

Table 6.4: Log in Threat Scenarios Results

1) *Log in using another participant's credentials*. In this case, the system automatically prevents the intruder from writing the information in the log in fields; this due to the face recognition procedure which decided that an unauthorised user is trying to log in.
2) *Using a full colour photo of a legitimate participant to log in* (e.g. a full colour 2D photo from a mobile device). None of the three participants succeeded in this attempt in either 2D or 3D mode.
3) *A legitimate participant accompanied with illegitimate participant trying to log in together at the same time to pass the face recognition barrier.* The system prevented this threat by recognising more than one face in front of the camera, and then the system prevented the intruder from writing the username and password/student number in the log in fields.

All results of the rest 9 threat scenarios (from 4 to 12) during the e-assessment are categorised and saved in the system database and images files. The following Table 6.5 summarises these results.

Threat	Continuous 2D and 3D Facial Recognition (FR) Identity Verification and System Security					
	2D FR Mode Identity Verification	**3D FR Mode Identity Verification**	**Head Movement Security**	**Eye Tracking Security**	**Speech Recognition Security**	**Multiple Face Security**
4	✓	✓	✓	✓	Not Applicable	Not Applicable
5	✓	✓	✓	✓	Not Applicable	✓
6	✓	✓	✓	✓	✓	Not Applicable
7	✓	✓	✓	✓	Not Applicable	Not Applicable
8	✓	✓	✓	✓	Not Applicable	Not Applicable
9	✓	✓	✓	✓	Not Applicable	Not Applicable
10	✓	✓	✓	✓	Not Applicable	Not Applicable
11	✓	✓	✓	✓	Not Applicable	Not Applicable
12	✓	✓	✓	✓	Not Applicable	Not Applicable

Table 6.5: Results of the 9 Threat Scenarios Repeated With 3 Participants

In the 2D mode, when participants left the location or chair, the camera captured no face in front of it; in addition, the eye tracker lost the eye movement information. While in 3D mode, the camera captured: no face, no head movements, no depth information, and no face expression information; in addition, the eye tracker lost the eye movement information. Figure 6.4 shows how each of these monitoring controls captured the absence of the participant from the chair.

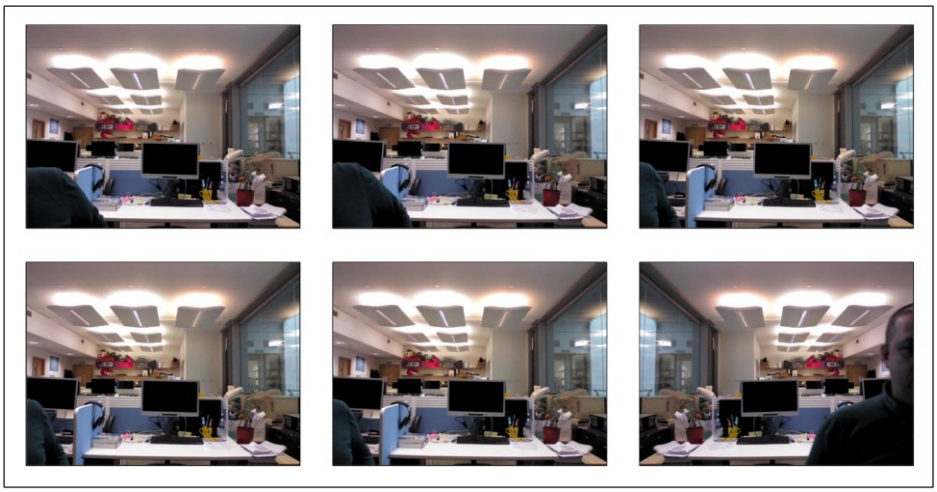


Figure 6.4: The Absence of the Participant from the Chair (No Face)

In the real implementation of the e-assessment, with this particular threat, in order to avoid recording a massive number of unnecessary misuse information (as there is no need to record any more information to provide evidence of cheating), the system can implement a time threshold (e.g. 20 seconds as the academic could see this time is more than enough to get unauthorised help) which represents the maximum period that the participant's face is allowed to be absent from the camera shot before logging the system out automatically and considering the case as an absolute cheating. This strategy can help to save the system resources and consequently enhance the operational nature of whole system.

In the case of using the keyboard, mouse, or the laptop mouse pad by somebody else, as presented in Figure 6.5, he should be close enough from the legitimate user to do this; the camera captured more than one face in both 2D and 3D modes.

Figure 6.5: Using the Keyboard, Mouse, or the Laptop Mouse Pad by Somebody Else (Multiple Faces)

In general, during the real test, the chance to capture two or more faces can be occurred from time to time depending on the surrounding environment, for instance, in a university lab where there are many people could overlap in the background of the captured image. Therefore, a minimum period of time (e.g. 3 seconds threshold) can be used to decide whether the more than one face in the captured image as a potential cheating attempt, in order to avoid recording and sending ordinary actions and consider them as misuse cases which might distract the academic in the reviewing and judging phase.

Furthermore, it is also possible to append additional policy when multiple face case occurred multiple times with the same strange face, the system could then more potentially consider them as misuse cases even though it lasts less than the predefined threshold. Moreover, as the e-assessment could be taken within the institutional examination centres, then it could be worth to define a list of exceptional or trusted faces (e.g. inspectors' faces) just in case if they would be captured in the background during the test, then the system should not consider this as misuse.

In the sixth threat scenario, further to the fact that every spoken sentence is recorded by the entire session recording process, once another individual answered the questions orally, the speech recognition algorithm captured every spoken sentence in both 2D and 3D modes (whereas the recognition system is continuously active during the assessment) relying on an English dictionary of the most 10,000 words used in English language, and if there is any spoken word or sentence by any person, which is picked up by the microphone, then it will be recorded and characterised by this recognition system as a potential attack. The system could

also improve its ability to detect users (more effectively) with a view to identifying misuse by a different strategy, for instance, if the case of the captured human speech accompanied with more than one face in front of the camera concurrently then the system would more probability consider this as a cheating attempt.

Fixing the camera and the eye tracker in front of the exam taker and moving the computer to another individual was the seventh threat scenario, the result has shown that it was very difficult to the participant to hold and handle both the camera and the eye tracker and mimic original locations. Therefore, the system captured misuse photos via both eye tracker (eye movements) and 3D camera head movement security subsystems. However, this particular scenario would not be able to be achieved easily in future planned development of the system, this due to the fact that the 3D camera (Intel RealSense technology) itself will be built-in most types of the computers as demonstrated in the previous chapter. Furthermore, the eye tracking security process can be accomplished utilising the same 3D camera, thus the current camera has the ability to provide this but the researcher has preferred to employ a separate eye tracker to achieve the highest level of accuracy.

In the case of turning the head to the left, right, up, or down (e.g. looking for unauthorised help from somebody else or reading a book or a text in mobile phone), as illustrated in Figure 6.6, they have completely been captured by Eye Tracker in the 2D mode, and by Eye Tracker in addition to the 3D camera relying on the head movements security strategy that were running together in the 3D mode only.

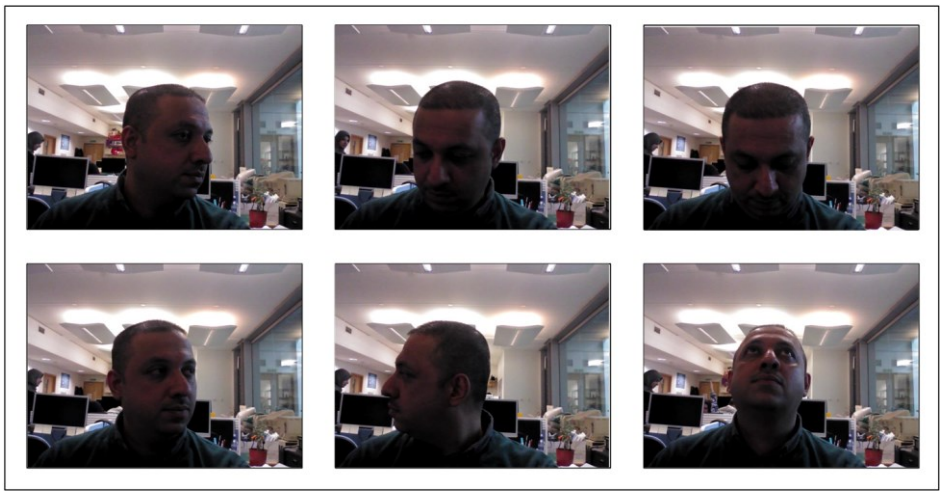


Figure 6.6: Example of the Capture by the Eye Tracker and Head Movements Security

Generally, throughout the actual test, it is usual that the student could move his/her head in different orientations from time to time. Therefore, it is advisable to define a minimum period of time (e.g. 2 seconds threshold as this would be enough time to get unauthorised help by looking outside the computer screen) can be used to decide whether the head motion in the captured image as a potential cheating attempt, in order to avoid recording and sending ordinary actions and consider them as misuse cases which might distract the academic in the reviewing and judging phase. Furthermore, the position of the face in front of the screen in these four different orientations could also be flexible and appropriate angles could be chosen among a range of maximum and minimum parameters. This could provide the system with a more flexibility in terms of considering the student's head within the acceptable position or not, and avoid sending a massive number of normal or legal face images for reviewing. Moreover, it is also possible to apply additional policy when this type of misuse occurred multiple times successively, the system could then more potentially consider them as misuse cases even though it lasts less than the predefined threshold (the allowed time). Additionally, in order to avoid recording a number of unnecessary misuse information, the system can implement a threshold time (e.g. 20 seconds as this would be the maximum period of time to get definitely unauthorised help by looking outside the computer screen) in which the participant's face is allowed to look outside the screen before logging the system out automatically and consider the case as a definitive cheating. This strategy can help to save the system resources and accordingly improve the overall operational nature of the system. However, with all the previous head movement potential security policies, if the student's eyes (according to the eye tracker monitoring) were looking continuously inside the screen boundaries then the head orientation can be given wider movement angles than the predefined limitations.

When participants have been asked to put a photo of a genuine exam taker in front of the camera (e.g. a full colour 2D photo from mobile device), the recognition succeeded for the majority of the samples which have been captured by the 2D facial recognition algorithm. However, they have been captured by Eye Tracker anyhow because there is no eye movement in the photos (as shown in Figure 6.7). In the 3D mode, the photos have been captured by Eye Tracker, in addition to the 3D camera via 3D facial recognition sub algorithm, because there is no depth and head movements information in this mobile 2D image.

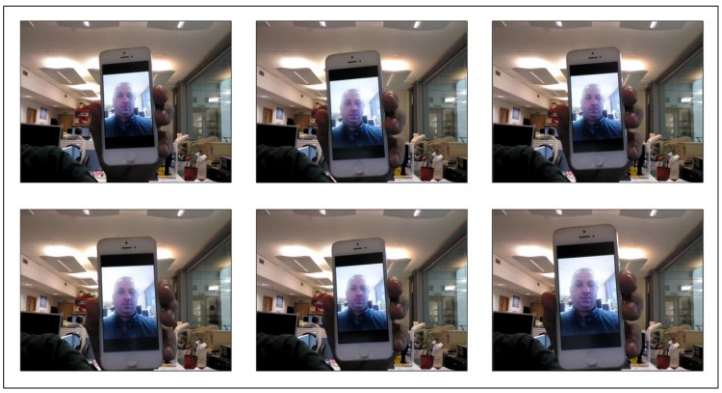


Figure 6.7: Using a Photo of a Legitimate/Genuine Exam Taker in Front of the Camera

The absence of eye movements in this specific attack makes all the values of eye tracking parameters to be zeros, which means no human in front of the computer screen and suggests considering this case as a definitive cheating. Therefore, similar to the first threat scenario, in order to avoid recording a huge number of dispensable misuse information, the system can also implement a time threshold which represents the maximum period that the participant's eye tracking information is allowed to be zero before logging the system out automatically and consider the case as an absolute cheating. This strategy can help to save the system resources and accordingly enhance the operational nature of whole system.

The same can be said for the tenth scenario, which was asking the participant to behave as intruder by using a photograph of the legitimate user as mask with eye holes to bypass the eye tracker challenge, the experiment results have shown that the holes should be much bigger than the original eyes in order to enable the eye tracker to reach the intruder's eyes. Nevertheless, because there is no depth and head movements information in these photographs, this particular attack, as shown in Figure 6.8, has completely failed in the 3D mode.

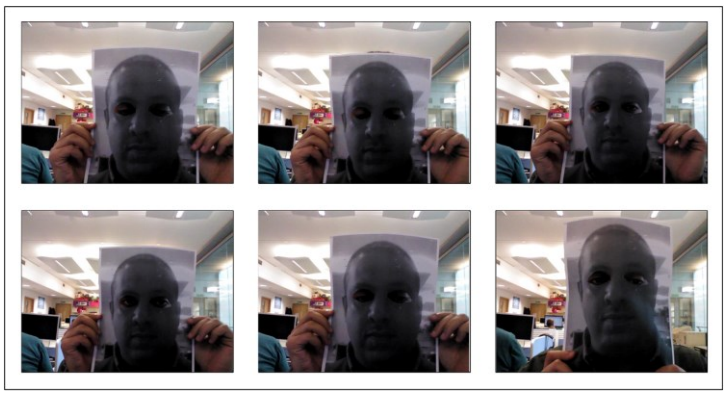


Figure 6.8: An Imposter Uses A 2D Photograph of the Legitimate/Genuine with Eye Holes

As the head movements security represents one of the system parameters that could be utilised to identify for sure the presence of the student in front of the computer/exam screen, therefore, the system could also implement a time threshold which represents the maximum period that the head movements information is allowed to be zero (no head movement recorded continuously during this period) before logging the system out automatically and considering the case as a definite cheating.

In the eleventh threat scenario, a participant has been asked to sit on behalf of the legitimate user, in both 2D and 3D modes the system easily highlighted there was another person in front of the camera. With this attack, a strict rule could be applied, as whenever illegitimate person sits the exam with a complete absence of the genuine exam taker, the system should treat this as a definitive cheating without any indulgence, therefore, the system could log out automatically after a short time, as there is no need to record any more information to provide evidence of cheating.

Finally, in order to examine the ability of the eye tracker infrared to penetrate the glasses and to explore whether the glasses have any direct impact on the facial recognition performance, as shown in Figure 6.9, the experimental result has proven that the eye tracker infrared beams were penetrating the glasses and achieved the same performance in the case of without wearing glasses, furthermore, it has also been proven that there is no direct correlation between the glasses worn by the participant and the performance of the facial recognition system. Essentially, when conducting the main experiment, just by a matter of fact, some of the 51 participants have been used some different glasses, however, the system has also proven the same results of this twelfth threat scenario.

Figure 6.9: Examples of Wearing dark glasses (2D Facial Samples)

Table 6.6 demonstrates the results of the 2D and 3D facial recognition FAR of the 5th, 9th, 10th, and 11th threat scenarios per participant.

Threat	FAR Results					
	2D Facial Recognition			3D Facial Recognition		
	Participant 1	Participant 2	Participant 3	Participant 1	Participant 2	Participant 3
5	0	0	0	0	0	0
9	0.076	0.076	0	0	0	0
10	0.038	0.076	0	0	0	0
11	0	0	0	0	0	0

Table 6.6: The 2D And 3D Facial Recognition FAR and FRR of All the Threat Scenarios per Participant

The results were zeros for all cases in both 2D and 3D facial recognition authentication, except the FAR of participants 1 and 2 of the 9th and 10th threat scenarios were 0.076, 0.076, 0.038 and 0.076 respectively in the 2D facial recognition mode. Then the best, worst and average FAR are summarised in the following Table 6.7.

Mode	The Best	The Worst	The Average
2D Facial Recognition Results	0	0.076	0.038
3D Facial Recognition Results	0	0	0

Table 6.7: The Best, Worst and Average FAR of the Three Participants in the Threat Scenarios

In general, the false acceptance rate in this phase is just for identification of how reliable the facial recognition system is, therefore, one of the reasons why it was not important to test with lots of people (more than 3 participants), because the purpose was not essentially to test the FAR or FRR. The FRR has previously been included in the usability analysis simply because if the legitimate person gets flagged up as illegitimate a lot of the time then the academic can have spent very long time reviewing images are perfectly legal, and that will represent a problem in the convenience and the usability of the system from the academic perspective.

6.4 Operational Considerations

This section will consider the third research question, as whether the system is able to scale appropriately to manage large volumes of examinees or not.

After completing the experiment, and across some discussions with the participants and conference audience, some people and experts were wondering whether the volume of the collected data including the database and the samples has been feasible or not. In terms of the operational aspects and the required space on the disk, the database size including all photos and Intel RealSense DB was 978.1 MB which whilst not a small volume of data is operationally within limits and demonstrates the ability to be scalable (into the order of hundreds (rather than thousands) of simultaneous assessments). Detailed data sizes are shown in Table 6.8, knowing that the size of each exam is 19.1 MB.

Categorizations	**Participants**	
	Per User	**All the 51 Users**
2D Samples	1 Every 4 Seconds (about 73), 2 MB	3723 Samples, 102 MB
3D Samples	1 Every 4 Seconds (about 146), 4 MB	7446 Samples, 204 MB
Audio Recording	12 MB	612 MB
Eye Tracking	0.6 MB	30.6 MB
Head Movements	0.5 MB	25.5 MB
Total Size	19.1 MB	974.1 MB + 4 MB For DB

Table 6.8: Complete Data Sizes

In the 2D mode, 73 facial recognition samples per user are captured on average, as no more than 2MB on disk is required for these samples per participant. A total of 102 MB of storage is used to store 3723 photos across all 51 participants. On average, the 3D facial recognition captured 146 samples per user. Less than 4MB on disk is required for these samples per user (the sizes of 2D and 3D facial recognition samples could be reduced if the academic decides to increase the period of taking the samples (e.g. > 5 seconds)). A total of 204 MB is used to store 7446 photos across all 51 participants. The recorded session (audio) was less than 12 MB per user and 612 MB for all participants. 30.6 MB is the total size of eye tracking security data in the whole experiment and about half MB for each user. The required space

for the data of head movements' security per participant is 500 KB and 25.5 MB for all of them.

In general, from a processing perspectives it is less time sensitive because the system follows a batch processing mechanism, therefore, it can take a long time to complete (it could take a day to come back that will be perfectly fine). What required is the system able to capture and store the information in real-time but the actual process in the biometric sample is not very important because the nature of the proposed processing itself solves/mitigates the problem as discussed previously.

The infrastructure of the proposed architecture of the system then would need to include three types of severs:

- A sever to be the web application,
- A sever to the backend processing, and
- A database server.

The above web application and database servers could be duplicated for the purpose of providing mirror servers for data redundancy in a worst case scenario. About 19 MB of data per student however can be considered a feasible to store this volume of data (the required space on the database server).

For example, in Plymouth University which is one of the largest universities in the UK, there are about 25000 students (HESA, 2017), if they took that test for 1 hour *(Four-fold the conducted online assessment time during the experiment)*; this could require:

19 MB (data size for 15 minutes) $\times$ *4 = 76 MB* per student for 1 hour.

Which means *76 MB* $\times$ *25 K = 1,900,000 MB (1.9 TB)* for all the 25000 students.

Therefore, this would cost the value of a local server with hard drive(s) < 2 TB, then the cost would be about *$ 750* (Dell, 2017). However, if the system has been enrolled for the cloud-based environment (Cloud Server), for the same volume of data, the cost would be about *$ 187.00* per month (Amazon, 2017).

In the UK institutions, students would typically take between 6 to 12 modules with some of these modules 0 or more tests, therefore, for easier calculation an average of 10 has been

assumed as possibly upper level of optional tests that would be taken during the entire academic year, then 19 TB *(10 x 1.9 TB)* must be available of memory space (local server with hard drive(s)) for the entire University online examinations per academic year. Then, this would cost in minimum about *$ 3800* (Dell, 2017). Thus, if the system has been enrolled for the cloud-based environment (Cloud Server), for the same volume of data, the cost of the storage then would be about *$ 900* per month (Amazon, 2017).

Both backend processing and the web application servers, on the other hand, would be quite small comparing with the database sever as all the collected data will be stored in it. Therefore, Table 6.9 illustrates in detail the estimations of the cost of these servers (Dell, 2017) depending on the collected data size per user (Table 6.8):

Server Type	Price	Mirror Price	Total
Web Application (e.g. 500 GB Server)	$ 620.00	$ 620.00	$ 1240.00
Backend Processing (e.g. 500 GB Server)	$ 620.00	-	$ 620.00
Database Sever	$ 3800.00	$ 3800.00	$ 7600.00
Total	$ 5040.00	$ 4420.00	**$ 9460.00**

Table 6.9: Estimated Servers Costs

On the other hand, for the same volume of data, if the system has been enrolled for the cloud-based environment, the cost then would be about as summarised in the following Table 6.10 (Amazon, 2017).

Server Type	Price Per Month	Mirror Price Per Month	Total Per Month
Web Application	$ 250.35	$ 250.35	$ 500.70
Backend Processing	$ 250.35	-	$ 250.35
Database Sever	$ 258.40	$ 258.40	$ 516.80
Total	$ 759.10	508.75	**$ 1267.85**

Table 6.10: Estimated Servers Cost in Cloud-based Environment

Generally, in order to use the available space effectively, reduce the final system cost, and improve the performance, compression techniques can be implemented on the stored data, which could reduce the sizes of the stored data particularly the sound files. However, the above estimated costs could be considered far less than employing hundreds of human inspectors (might be untrusted or inexperienced) to achieve the monitoring process on this numerous number of online examinations that should be taken inside the University using its

resources including the electricity, computers, equipment and all other infrastructure that would be required to accomplish every test (this will definitely cost the University further huge amounts of money). For example, in Al-Quds Open University (QOU), for 7000 students in one educational region in the first and the second terms 2010/2011, Sabbah et al., (2012) showed that 50 proctors per session are required in 36 sessions with around $20 per session, in a total cost of $36,000 per term for one region. Therefore, the annual cost for proctors in QOU would be $1.5 million.

The calculation of the bandwidth per user for such system is:

19 MB = 19 x 1024 x 8 = 155648 Kbit

As the exam time during the experiment was *15 minutes = 15 x 60 = 900 sec*

Then, *155648 Kb / 900 seconds = 172.94 Kb/sec* the bandwidth required per user

If the student takes the test in one of the University examinations centres, and if the network speed was 100 Mb:

100 Mbit = 100 x 1024 = 102400 Kb

Then *102400 Kb / 172.94 Kb/sec = 592* the maximum number of student that can take concurrent connection (i.e. it takes all the network bandwidth (capacity)). However, as discussed previously (Chapter 4), the system administrator has the ability to setup a maximum number of concurrent users (e.g. 100 students).

On the other side, if the student takes the test from outside the University, and if the Internet speed was for instance 100 Mb/sec, then the maximum number of students is also 592 based on the same 172.94 Kb/sec of bandwidth calculated. Therefore, regarding the cost, if the system has been enrolled for cloud-based environment, for the 1.9 TB of data with this bandwidth, then the traffic of all the 25000 students in the University would cost about $*169.65* per month (Amazon, 2017), thereby, the annual cost would be $2035 (*12 x $169.65).* This is a very small cost comparing with the total cost calculated in the above example of QOU, which is $1.5 million (for only 7K students), whereas this system calculation has been done base on about 3.6 times of this number (25K students) which means it would cost $5.4 (*3.6 x $1.5)* million per year for physical proctors.

6.5 Discussion

Due to its transparency and reliability, Intel RealSense face recognition technology has been chosen to be the main authentication approach in this e-invigilation system. Beyond the former modality, many of the other proposed biometric modalities can be utilised to enhance the performance. For instance, the low-cost mouse movements and keystroke recognition, which could provide a high level of transparency and usability; in addition to their encouraging implementation especially in the case of combining them with other biometric techniques, such as linguistic analysis. However, more work is required on those modalities to get them to the point of being reliable and implementable within this system.

Both eye tracking (left eye, right eye, and the centre point of 30 sample every second), and head movement information (Roll, Yaw, and Pitch of 3x25 samples every second) are continuously measured and recorded in every test during the experiment. This could give the opportunity to explore the possibility of proposing these collected data to be employed to produce a novel and new behavioural biometric modalities (namely: Eye and Head Movement biometric modalities), thereby can be utilised as additional non-intrusive and feasible biometric modalities to improve the authentication performance. These eye and head movements are unconscious human behaviour which means the people cannot feel anything when they occur, this fact puts these techniques on the top of the most transparent biometric modalities list, and can be collected even without the user knowledge.

During the experiment, participants' left and right eye images are collected by the custom software, as demonstrated in Figure 6.10, this occurs in the registration stage using the 3D camera, which opens the door for utilising these images (after enhancement processes perhaps) for iris recognition as an additional strong biometric modality to the system. Iris recognition offers an interesting opportunity as it is generally considered a highly reliable modality with robust performance. However, research has not thoroughly investigated to what extent a partial iris image is useful in providing identity verification and to what degree of performance, therefore, further research needs to be done looking at the use of iris recognition and also the iris recognition of partial iris.

Figure 6.10: Example of Captured Photos of Each of the Left and Right Eyes

These photos have been extracted (clipping rectangles around the eye areas) from the participant's 2D face image that has been taken in the registration/enrolment stage.

The use of an eye tracker in the experiment was interesting as it is an effective, efficient and reliable technique. However, current implementations still require a sensitive near-infrared cameras/sensors in order to achieve the eye tracking process. However, the 3D camera has further functionality that could also enable eye tracking process which can be considered promising as this type of technology and particularly the 3D camera will be seeing to be integrated widely (as discussed previously in Chapter 5) into consumer hardware devices, therefore it is more likely that all the hardware and software that the proposed system need will be included/installed within the devices by default in future. In order to enhance the overall performance of the continuous identity verification system, the collected and saved eye movements information (using the eye tracking security system), as discussed in section 3.4.2.5.1, can be utilised to produce promising new and very transparent biometric modality as it is one of the biometrics that can be collected from the face area without any direct connection or even without the student knowledge (passively).

In both 2D and 3D modes, the speech recognition algorithm captures every spoken sentence relying on an English dictionary. A subroutine called "Language Selection" has been developed and can be fetched by clicking the Language Selection button (as depicted in previous chapter Figure 5.19), which enables the system administrator to easily change the size*/type of the dictionary according to their need. Since the recognition algorithm can be applied on any language, the dictionary language is not restricted to English, the system users can choose any language they would like (e.g. French, Arabic or Chinese dictionary). As long as it captures the speech start and end, then the duration for each spoken sentence can be calculated. Therefore, in the case of any unauthorised talks that would happen during the e-assessment, this will give the academic a chance to listen to those particular short periods rather than the whole session. Furthermore, these captured sentences can be used to facilitate utilising linguistic analysis or even can be utilised for voice verification purposes as further

transparent biometric modalities. Moreover, in such recognition system, the academic can predefine a particular set of words to be included in the security subsystem in order to match them with the words of the captured sentences; this would help to normalise, prioritise, and consequently enhance the captured and reported cases of speech recognition misuse. For example, if the test is database systems, then the academic can predefine a group of words (e.g. SQL, Attribute, or DBMS) that could be considered more commonly used when talking about database system examination, then the system could prioritise presenting these particular sentences as misuse actions over the other sentences.

The scenario of running such system would differ with the other kinds of huge online learning platforms (i.e. the Massive Open Online Course (MOOCs) – online course aimed at unlimited participation and open access via the web). For instance, in such systems there might be thousands of people sitting for assessment at the end of the course. Therefore, it is obvious that the nature of the underlying architecture would significantly need to increase in order to cope and deal with such vast volumes of concurrent connections, this should use concurrent connections because when someone sits the test, typically in many cases, the assessment regulation requires all students of that module might be sitting test at the same time. Essentially, the system was not designed with MOOCs in mind first instance and actually a lot more further work would need to be done looking at the nature of the enterprise infrastructure required to support this, because obviously with that number of concurrent people that schedule in different times this system would struggle as a lot of information coming and being processing simultaneously, however, there is no reason why this would not scale with such massive enterprise architecture of huge physical data centres (MOOCs).

** The size of the dictionary (or the number of words) is dynamic and can be changed easily via the same Language Selection subroutine according to the academic's desire. For instance, during the experiment, the researcher decided to use an English dictionary with the most used 10.000 words in the English language.*

6.6 Conclusion

The chapter has experimentally explored the viability of a more secure, transparent and continuous authentication mechanism for e-assessments, which proposed in Chapter 4 of this thesis. The core research questions have been answered experimentally involving a

significant number of real participants over a reasonable period of time of real online assessment employing the previously developed prototype.

The experiment results have proven the ability of the proposed system to capture, process, and identify users through the use of biometrics. The achieved FRR has validated to a great extent the usability of the system and its ability to correctly recognise the legitimate user utilising the facial recognition in 2D and 3D modes under normal use. The results in this context have also demonstrated that the participant's face expressions (e.g. smile or eyebrow down) play no role in the recognition performance. Furthermore, the other factors have also no effect on the facial biometric recognition performance, such as wearing glasses or head veil during the regular experiment test time. The capturing mechanism has been accomplished transparently during the entire 51 controlled e-assessments with a reliable biometric sampling process.

The inclusion of additional biometric modalities (e.g. iris recognition, scar and mole identification, or mouse movement) in the theoretical architecture would deal with some threat scenarios (e.g. identical twins or even the face veil that some people would wear) that the 2D and 3D facial recognition algorithms in the current developed and utilised prototype would not be able to recognise. However, the results of the implemented threat scenarios have perfectly shown the capability of the suggested approach to identify, track, and monitor users with a view to identifying unauthorised help that could be provided by somebody else during the e-assessment. The resulted FAR has proven that the participant biometric modality could not be forged by illegitimate users. Furthermore, experimentally, the employed security restrictions including eye tracking, head movements, speech recognition, or multiple face detections have been perfectly identifying all the misuses which have been done as predefined threats by the three participants group.

Finally, from the cost perspective, the operational nature of whole architecture and its cost estimations in both system- and cloud-based servers have shown that they could be considered feasible.

7 Evaluation of the Proposed Approach

7.1 Introduction

The purpose of this chapter is to achieve a series of scenario-based stakeholder evaluations to provide a comprehensive understanding into the effectiveness of the proposed approach. Despite the promising validation results obtained in the in Chapter 6 of the thesis, there is a need for an additional qualitative and quantitative evaluation by the core stakeholders of the system. As it has previously been identified (in Chapter 5), academics and students are the main stakeholders of the system, therefore, their opinions on the system are essential. Furthermore, there is a need to consider experts in the field of the e-learning and information security in order to provide a more accurate scientific judgment on the proposed system and to better understand the acceptability and usability of the proposed system.

7.2 Methodology

Selecting suitable research methods is very important as the wise choice will lead to provide answers to the research questions accurately, in contrast, if the research methods are not suitable, the results will be inadequate (Ishak and Alias, 2005). There are two approaches to conduct a research namely: qualitative and quantitative approach (Howell, 2013).

Qualitative research is mainly investigative research. It is used to gain an understanding of fundamental reasons, opinions, and motivations (Given, 2008). It is also employed to expose trends in thought of individuals, and dive deeper into the problem. The data collection in this approach varies using unstructured or semi-structured techniques including: focus groups, individual interviews, and participation/observations. Typically, the sample size is small, and respondents are chosen to accomplish a given quota (Alasuutari, 2009). This approach has been used as a primary method in this evaluation, therefore, the respondents selected to participate in this research are comfortable with the qualitative approach. On the other hand, the research also utilised the quantitative method, generally, it is employed to quantify the problem by means of creating numerical data or data that can be converted into usable statistics (Franklin, 2013). It is utilised to generalise results from a larger sample population (e.g. a group of tens of students as subset of thousands in the university). The data collection in quantitative approaches methods is much more structured than the data collection in qualitative approaches. It includes: online surveys, paper surveys, mobile surveys, face-to-

face interviews, telephone interviews, longitudinal studies, website interceptors, online polls, and systematic observations (Creswell, 2013).

Phenomenology is the study of experience and how humans experience. It studies structures of conscious experience as experienced from a subjective or first-person point of view (Giorgi, 2009). As the individuals generate their own thoughts through their interaction with others in their communities, it is impossible to measure human behaviour without bias. In this research the designed questionnaires, for all groups, contains open-end questions that provide the participant the opportunity to express their opinions on the weaknesses/limitations of the system and another question was included to give them chance to suggest any recommendation they would like. For each particular question, the qualitative responses of all participants are grouped within one paragraph in order to provide consolidated narrative regarding a specific idea and to compare between different respondents' perspectives on the system.

To evaluate all dimensions of the EIEA system, the three separate stakeholders got three separate sets of information and three separate sets of questions, in two cases it is a qualitative-based survey (experts and academics) and the other one is a quantitative-based and qualitative-based survey (students). The richness of experts' responses is far larger than a tick box question. The academics can also provide detailed responses, and they have the largest interaction with the system. Therefore, a qualitative-based survey would be more suitable for both groups. However, when it comes to students, essentially what they interact with is relatively minimal, so in terms of having a qualitative, there is not much that would be asked. The questions would be about the students' desire to use biometric-based systems, their understanding with respect privacy, and to understand whether the enrolment process is simple enough for them to take. Therefore, a quantitative-based survey would enable to achieve all of that. And also doing quantitative allows getting a large group of people that allowed the researcher to get a wide set of students.

The main reasons/benefits for additional qualitative evaluation can be summarised as follows:

- To evaluate the identified research problem.
- The value of utilising continuous and transparent authentication in e-invigilation of e-assessments.
- To evaluate the feasibility, achievability, and practicality of the method.

- To evaluate the transparency and robustness of the proposed biometric modalities in the developed system.
- To evaluate the security provided by the system.
- To evaluate the security provided in terms of minimising the opportunities of cheating threats.
- To ensure whether the robustness of the developed system enables it to completely replace the position of a physical/human invigilator or not.
- To evaluate the robustness of the experimental validation of the approach.
- To identify the strengths and weaknesses of the developed system.
- To identify the key barriers moving forward.
- The attractiveness of the format and layout of the system interfaces.
- To evaluate the interfaces that enable the academic to create, view, and edit exams.
- To get the evaluation about how interfaces allow the academic to quickly identify and judge cases of misuse.
- To get the evaluation about the information given by the academic system perspective.
- To estimate whether the system allows finding and identifying the individuals in large groups that the academic suspects might be cheating in a timely fashion.
- To estimate to what degree the developed system might be able to completely replace the position of a physical/human invigilator.
- To get suggestions in order to integrate anything might be missed from the system.
- Research novelty.

Furthermore, the main reasons/benefits for additional quantitative evaluation (*that has been dedicated to the students' group*) can be summarised as follows:

- To evaluate the security, privacy, transparency, and convenience provided by the system login process.
- To evaluate the design, colours, and usability of the format and interfaces of the system.
- To evaluate the ability of the system to detect cheating, applied over the Internet, take the position of the physical invigilator, and applied on a range of devices (e.g. Mobile).

- To evaluate the robustness and convenience of the biometrics and security monitoring that used in the proposed approach.
- To get the student's evaluation regarding the comfortability, privacy, and the system immunity against spoofing actions and effectiveness to be utilised for continuous authentication purposes of specific biometric authentication approaches including: 2D facial recognition, 3D facial recognition, mouse dynamic analysis, keystroke analysis, eye movements, head movements, linguistic analysis, iris recognition, fingerprint recognition, and retina recognition.
- To evaluate student's comfortability, privacy, transparency, and convenience with respect to recording all the surrounding sounds during the test for security purposes.
- To understand the student's feeling regarding involving the new technologies that enhance the monitoring process.
- To get a general idea about the students' thoughts (comfortability, necessity, security, and convenience) behind the idea of having monitoring.
- To get the student's opinion about comparing traditional invigilation with e-invigilation in terms of comfortability, necessity, security, and convenience.
- To get the student's feeling about the complete room checking that would be done by most commercial proctoring systems via the webcam, in terms of comfortability, necessity, security, and convenience.

For a qualitative perspective, a one to one interview or Skype meeting has been carried out with each expert in order to get a more comprehensive evaluation in terms of exploring the wider aspect of the system, the use of the biometrics for the system security, the monitor, or the use of the storage. Asking the academics' group to evaluate the system through interviewing (if possible) or sending them the questions in order to provide the answers on a paper or electronically at their convenience to give them enough time to review and then judge the system fairly. Moreover, from both a quantitative and qualitative perspectives, the students' group has been asked to answer questions electronically (over the Internet) as it is the best way to get the largest number of students from a range of different field of studies across different countries, as in reality they are the largest group of stakeholders so the researcher decided to collect the largest number of quantitative responses.

7.2.1 Preparation of Interviews/Questionnaires

The questionnaires/interviews design stage included the following steps:

- Questionnaire design.
- Specifying the questions, the number of questions, and the number of interviewees within each separate stakeholder groups.
- Interviewee search and selection/recruiting.

In order to develop clear and none overloaded questionnaires, the most important qualitative and quantitative evaluation questions for the PhD research were asked. Throughout the questionnaire design phase, it was challenging to balance between the evaluation objectives of the interview/questionnaire and an easy and quick to understand/answer format.

In order to evaluate the novelty, feasibility, acceptability, usability, privacy, and practicality of the research (evaluation all dimensions of the EIEA system), the questionnaires adopt achieving qualitative-based and quantitative-based survey by asking three separate sets of questions. Therefore, given the previously identified research objectives, the following are series of a variety of questions that have been derived from intensive analysis to the system environment.

7.2.1.1 Experts' Questions

Eleven open-ended qualitative questions for the Experts' group set of questions were drafted taking into account the target of achieving the survey aims, being understandable by different experts, being objective, and being answered in an average of 35 minutes by the chosen participants.

The first question aims to gather information about the experts' viewpoint on the value of the identified research problem by asking:

- What are your thoughts about the identified research problem?

One of the most important objectives of the approach is to achieve the idea of utilising continuous and transparent authentication in e-invigilation of e-assessments, it is expected that the answers to the following question will show the contribution and novelty of this idea.

- What do you think about utilising continuous and transparent authentication in e-invigilation of e-assessments?

To ensure about the feasibility, achievability, and practicality of the method, the third question has been asked:

- To what extent do you think it is feasible/achievable/practical?

To evaluate the transparency and robustness of the proposed biometric modalities in the developed system the experts had answered the following question:

- To what extent do you think the proposed biometric modalities in the developed system are transparent and robust?

The fifth and sixth questions are dedicated to emphasise the value of the security provided by the system and its role to minimising the opportunities of cheating threats.

- What do you think about the security provided by the system (e.g. eye tracker)?
- To what extent do you feel the security provided can help to minimise the opportunities of cheating threats?

The answers to seventh question should help to get the experts' opinion about whether the robustness of the developed system would enable it to completely replace the position of a physical/human invigilator or not:

- To what extent do you think the developed system is robust to enable it to completely replace the position of a physical/human invigilator?

It is expected that the answers to question eight could provide evaluation of the experimental validation robustness of the approach

- To what extent do you feel the experiments have provided a robust validation of the approach?

To identify the strengths and weaknesses of the developed system, the following question nine was asked:

- What do you feel are the particular strengths & weaknesses of the developed system?

To get the experts' anticipation about a potential limitation, question ten was aimed at exploring and identifying the key barriers moving forward:

- What do you feel are the key barriers moving forward?

To give the experts the opportunity to express their opinions, ideas or suggestions about the developed project or the entire research and every proposed idea behind it, the questionnaires ends with the closing question:

- Is there anything else you would like to add?

7.2.1.2 Academics' Questions

A set of 9 open-ended qualitative questions for the academics' group of questions were drafted taking into account the target of achieving the questionnaire aims, being understandable verity of academic, being objective, and being answered in no more than 35 minutes by the participants.

The first to the fourth questions are dedicated to evaluate the academic interfaces in terms of the format, layout, ease of use (e.g. creates, view, and edit exams), and how much it would quickly identify and judge cases of misuse:

- What do you think about the format and layout of the interfaces?
- How do you feel about the interfaces that enable the academic to create, view, and edit exams?
- To what extent do you feel the academic interfaces allow you to quickly identify and judge cases of misuse?
- Does the academic subsystem give you the information you need? If not, what is missing?

It is expected that the answers to question five could provide the academics' estimation about whether the system allows finding and identifying the individuals in large groups that the academic suspects might be cheating in a timely fashion.

- Thinking in particular of large groups (c.200+) would the system allow finding and identifying the individuals that you suspect might be cheating in a timely fashion?

The answers to the sixth questions should help to get the academics' opinion about whether the robustness of the developed system would enable it to completely replace the position of a physical/human invigilator or not:

- To what extent do you think the developed system is robust to enable it to completely replace the position of a physical/human invigilator?

Question seven was aimed at gathering academics' suggestions in order to integrate anything might be missed from the system.

- Would you like to suggest anything you feel is missing from the system?

To identify the strengths and weaknesses of the developed system, the following question was asked:

- What do you feel are the particular strengths & weaknesses of the developed system?

To give the academics the opportunity to express their opinions, ideas or suggestions about the developed project or the entire research and every proposed idea behind it, the questionnaire ends with the closing question:

- Is there anything else you would like to add?

7.2.1.3 Students' Questions

The survey was structured to contain fifteen quantitative closed-ended questions in addition to one qualitative question (the 16th) comprising a variety of Likert scale with an option for the respondents to comment in the last question where the question is opened-ended. However, respondents were not obligated to answer all questions. This set of questions was drafted taking into account the target of achieving the questionnaire aims, being understandable by verity of students in different fields of study, being objective, and being answered in average of 20 minutes by the students' group participants (to read the questions, please see electronic Appendix C).

Question one was asked to gather the students' opinion on the security, privacy, transparency, and convenience provided by the system login process.

Question two was asked to get the students' evaluation regarding the design, colours, and usability of the format and interfaces of the system.

Question three was aimed at evaluating the ability of the system in terms of detecting cheating, the possibility to be applied over the Internet, to take the position of the physical invigilator, and to be used on a range of devices (e.g. Mobile).

It is expected that the answers to question four and five could gather the students' evaluation about the robustness and convenience of the biometrics and security monitoring that used in the proposed approach.

The answers to the sixth to ninth questions should help to get the students' opinion about the student's comfortability and privacy regarding employing particular biometric authentication approaches including: 2D Facial Recognition, 3D Facial Recognition, Mouse Dynamic Analysis, Keystroke (keyboard) Analysis, Eye Movements, Head Movements, Linguistic Analysis, Iris Recognition, Fingerprint Recognition, and Retina Recognition. Furthermore, these questions are dedicated to gathering student's opinion about the level of immunity against spoofing actions of these approaches, in addition to the effectiveness to be utilised for continuous authentication purposes.

The tenth question was dedicated to gather students' opinions about the comfortability, privacy, system transparency and convenience with respect to recording all the surrounding sounds during the test for security purposes.

To get the student's opinion about the comfortability, transparency, necessity, convenience and feasibility of new technologies such as the cameras/sensors with infrared lights to be employed in order to enhance the monitoring process, the eleventh and twelfth question were asked.

The answers to the thirteenth question should help to get a general idea about the students' thoughts (comfortability, necessity, security, and convenience) behind the idea of having monitoring.

It is expected that the answers to question fourteen could gather the student's impression about traditional invigilation comparing with e-invigilation in terms of comfortability, necessity, security, and convenience.

Question fifteen was asked to get the student's feeling about the complete room checking that would be done by most commercial proctoring systems via the webcam, in terms of comfortability, necessity, security, and convenience.

This questionnaire ends with the closing question "Is there anything else you would like to add?" to give the students the opportunity to express their opinions, ideas or suggestions about the developed project or the entire research and every proposed idea behind it.

7.2.2 Questionnaires' Participants

After defining the number of interviewees for each stakeholder group, the search for the interviewees began. In general, experts and academics with good educational background knowledge are desirable due to the educational context of the research in order to ensure gathering feedbacks which are adequate for PhD research. Furthermore, in order to better cover all dimensions of the offered research, the computer science point of view is also essential because of the computing context of the research (biometric authentication and system/information security).

The search process of the experts was realised via the Internet (e.g. LinkedIn social network, related conference keynotes, and university related departments) as follows:

- Members of committees thematically related to the research area of scientific conferences.
- Authors of work thematically related to research articles in scientific journals.
- Scientists from related fields working also as lecturers and/or as administrative staff members in e-learning or educational technology field.

This research was aiming to get the 12 experts in e-assessments, e-learning, or distance-based learning, 12 are considered a sufficient baseline to have in order to obtain the necessary perspectives from research and practitioner based experts, as prior literature overview revealed the ranges usually include up to ten persons for the qualitative evaluation of research: 6 persons (Creswell, 2007), 6-8 persons (Kuzel, 1999) and 6-10 persons (Morse, 2000). However, the lowest response rate, unfortunately, was in the experts' group (only about 6% of the invited experts had responded – 81 invited; 5 interviewed; 16 apologised; 11 responded to the basic invitation but did not accomplish the interview; 49 did not respond to the invitation at all). This might due to the fact that most of the invited experts are university staff members (professors, or associate professors) and the invitations were sent to them in August, when most of them were on annual leave until September, this could be an additional factor in diminishing the response rate among this particular group, nevertheless, the invitation has been sent twice or more to most of those who did not respond. Generally, it

was not an easy job to find and contact 81 experts around the world have experiences in e-learning and fair knowledge in the field of information system security and biometric technologies at the same time.

Furthermore, ten university academics (e.g. PhD researchers or staff members) were also targeted to provide additional evaluation by answering qualitative questionnaire as well. 50% of the selected and invited academics had responded and participated in a reasonable time. All of them are PhD students in the UK universities, they are practicing academics who teach or actively engaged in teaching and research in other institutions. However, the researcher interviewed 14 academics which is more than the basically targeted number.

In a far higher and faster response, 44 participants (which is more than the targeted 30 participants) of the students' group have responded recording the highest response rate among the three stakeholder groups with about 80% of the invited students. All of them are undergraduate students in various universities.

In the case of experts interviews, the questions were asked as paper-based in the case of interviews in written form, were sent to them via the email to be answered (e.g. Word/PDF file) even without conducting the interview, or were asked directly in the case of face-to-face/Skype interviews.

In the case of academic, the interview was conducted face-to-face at participants' locations. The questions were asked directly. However, most of the academics gave their answers to the questionnaires in written form.

On the other hand, the questions were sent via email to every participant in the students' group, the questions have been asked as paper-based in written form. They gave their answers to the questionnaires in written form.

In order to be able to take part in this study, only participants who are 18 years old and above, agreed and understood all procedure, the targeted stakeholders:

7.2.2.1 Experts

Five experts were interviewed to evaluate the devised approach to electronic invigilation that provides the monitoring and controls required to remove the necessity of having a physical proctor. They are from different countries around the world. All of them are specialists in the felid of e-learning and distance-based learning, three of the interviewed experts have extensive knowledge in the field of computing (PhD /M.Sc. /B.Sc. in computing) and all of them have educational/teaching backgrounds.

Experts have been formally invited (from inside or outside Plymouth University – i.e. from different countries around the world) either in person or via e-mail. Once an expert initially accepted the invitation the consent form has been sent to him/her to sign. A summary of how the system works including screenshots of the interfaces, consent form, question list and information sheet has also been emailed to the expert prior to the interview (see Appendix A). They have been then asked to suggest the convenient way of conducting the interview (i.e. face-to-face or answer the questions electronically). A demo of the system has been presented to the interviewee (a 20:46 minutes video was dedicated for the experts' group www.youtube.com/watch?v=rr6wFdaNqvU&t=1105s), the video presentation started as a slide presentation with an audio podcast, it also could be watched on YouTube as this could enable the expert to speed it up, avoid the download, and get a higher resolution. Then they have been asked to suggest the comfortable time for conducting the interview. All the session have been recorded (i.e. recording the entire Skype interview using special recording software) after having a permission of the interviewee and transcribed afterwards. All interviews were conducted in English to avoid translation bias. The total amount of time needed for each expert participant has been ranged between 30 to 35 minutes depending on the questions and the discussion.

In general, although the face-to-face or Skype interviews were the best choices due to they give more detailed and personal conversation, but the formal written interview format also has some benefits including clearer, more formal, more focused answers at the interviewee's convenience, avoiding scheduling strict date and time, and greater ease of interview processing and storage. One expert provided his answers to the questionnaires in written form after the Skype interview. However, the rest four experts agreed to provide face-to-face/Skype interviews and answer the questions directly (all the experts' interviews can be found in electronic Appendix D). Please see Appendix A for ethical approval notifications.

For more details about their experiences and research focuses, the following list provides a summary abut each expert:

- Steve Wheeler is Associate Professor of Learning Technologies at the Plymouth Institute of Education where he chairs the Learning Futures group and leads the Computing and Science education teams. He researches technology supported learning and distance education, with particular emphasis on the pedagogy underlying the use of social media and Web 2.0 technologies, and also has research interests in mobile learning and cyber cultures. He has given keynotes to audiences in more than 35 countries and is author of more than 150 scholarly articles, with over 5000 academic citations. He is an active and prolific edublogger, and his blog Learning with 'e's is a regular online commentary on the social and cultural impact of disruptive technologies, and the application of digital media in education, learning and development. In the last few years it has attracted in excess of six million unique visitors.

- Akinori Nishihara received the B.E., M.E. and Dr. Eng. Degrees in electronics from Tokyo Institute of Technology in 1973, 1975 and 1978, respectively. Since 1978 he has been with Tokyo Institute of Technology, where he is now Professor of Human Assets Promotion Project for Innovative Education and Research (HAPPIER). His research interests are in signal processing and educational technology. He published more than 300 technical papers in refereed international journals and conferences. He received IEICE Best Paper Award (1999), IEEE Third Millennium Medal (2000), Distinguished Service Award for IEEE Student Activities (2006), Tokyo Tech Best Teacher Award (2009), Tokyo Tech Best Engineering Teacher Award (2013), IEEE Region 10 Outstanding Volunteer Award (2015), and Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology (2016). He is an IEEE Fellow, an IEICE Fellow, and a member of AACE, APSIPA, and JSET.

- Minoru Nakayama is a Professor at Information and Communications Engineering, Tokyo Institute of Technology, Japan. In 1983, He completed Bachelor's Degree in Education at Department of Education, Tokyo Gakugei University, the Master of Education program in 1985, and received a Doctor of Engineering degree from Tokyo

Institute of Technology in 1990. His research concerns Human Visual Perception and Educational Technology. He is a member of: The Japan Society for Educational Technology, The Institute of Electronics, Information and Communication Engineering (IEICE), The Japanese Psychological Association, The Institute of Image Information and Television Engineering (ITE), The Institute of Electrical Engineers of Japan (IEE), The Japan Society for Science Education, The Chemical Society of Japan, and The British Educational Research Association (BERA).

- Peter Bryant: a creative technology and education leader, with a clear vision for enhancing the student experience. He engages widely and critically with emerging trends and transformative practices to help shape the direction of teaching, learning and innovation. Mr. Bryant develops an innovative and agile culture of experimentation and play. He is a supportive and critical leader in terms of change management. His experience can be summarised as: Head of Learning Technology and Innovation (The London School of Economics and Political Science (LSE) January 2014 – Present (2 years 9 months) London, United Kingdom), Strategic direction of teaching, learning and technology, Innovative and agile use of social media, Change management, Leading transformation of practice, Institutional governance and strategic leadership of key projects, and Creative innovation management.

- Dr Jekaterina Rogaten is a research associate at the Institute of Educational Technology at the Open University UK and also holds lectureship position in positive psychology at the College of Fashion, University of the Arts, London. Her main research interests are in learning analytics and in positive psychology with a particular focus on learning gains, performance, progress, approaches to studying, creativity, metacognition and emotions. Jekaterina published in National and International journals and presented at European and International conferences.

7.2.2.2 Academics

14 academics were interviewed to evaluate the suggested system. The academics' group is heterogeneous; it consists of academics/lecturers from different areas of studies (including computing (7), engineering (4), pharmacy (1), English literature (1), and mathematics (1)) and different nationalities. All interviewees have a research background. They are all

lecturers with several years of experience in various universities, which is also vital in the scope of the electronic learning context of this study. Diverse perspectives from academics with different backgrounds and fields help to provide a variety of opinions on the offered approach. Due to the computational context of the research (biometric authentication and system/information security), the majority (7 have PhD/M.Sc./B.Sc. in computing) of the invited academics have extensive knowledge in the field of computing.

They were formally invited (from inside or outside Plymouth University – i.e. from different Universities within the UK) in person, via e-mail, or by messages/call through social media (e.g. Facebook). Once an academic initially accepted the invitation, an email has been sent contains a summary of how the system works including screenshots of the interfaces, consent form to be signed, question list, information sheet, and a demo of the system (11:55 minutes www.youtube.com/watch?v=rc3we4zk2WY&t=2s), the video has been presented to them in the same way as with the experts.

Then they were asked to suggest the time of conducting the interview. In the case of the interview, all the session has been recorded (i.e. recording the entire interview using mobile phone recording application) after having a permission of the interviewee and transcribed afterwards. The interviews were conducted in English to avoid translation bias. The total amount of time needed for academic participant has been ranged between 30 to 35 minutes depending on the questions and the discussion.

All of the academics provided their answers to the questionnaires in written form, with the exception only one academic agreed to provide a face-to-face interview that recorded using a mobile phone recorder, this interview was transcribed afterwards (all the academics' interviews text in electronic Appendix D).

7.2.2.3 Students

Ultimately 44 students were surveyed in this system evaluation process. The students' group is also heterogeneous; it consists of students from different areas of studies (e.g. computing, engineering, and mathematics). They are from different stages in various universities. Diverse perspectives from students with different backgrounds and fields help to provide a variety of opinions on the offered approach. Due to the computational context of the research (biometric authentication and system/information security), the majority of the invited/participated student have very good experiences in using of computer.

They have been formally invited (from different Universities around the world) in person, social network, or via e-mail. Once a student initially accepted the invitation, an email has been sent contains a summary of how the system works including screenshots of the interfaces, consent form to be signed, question list, information sheet, and a demo of the system (6:22 minutes www.youtube.com/watch?v=Vf3SGU_b12I&t=246s), the video has been presented to them in the same way as with the other two stakeholders. All the students provided their answers to the questionnaire in written form (all the students' interviews text in electronic Appendix E). To avoid translation bias, all questionnaires were accompanied in English.

In general, as stated in the consent form, all the participants in the above 3 groups were free to withdraw from the research, and ask for data to be destroyed if they wish (at any time during the interview session or information/feedback collection process).

7.3 Results

This section presents the outcomes of the three questionnaires/interviews. Moreover, the qualitative/quantitative point of views of the experts, academics, students are highlighted and discussed here.

7.3.1 Outcomes of the Experts' Group interviews

The interview with Associate Professor Steve Wheeler was face-to-face and recorded using a mobile phone recorder. The interviews with Professor Akinori Nishihara, Mr Peter Bryant and Dr. Jekaterina Rogaten were via Skype and recorded using MP3 Skype recorder. These interviews were transcribed afterwards. There was no need to transcribe the recorded Skype interview with Professor Minoru Nakayama, as the interview was dedicated for a long discussion between the interviewee and the researcher about the research problem and many subjects related to the project and the research area, and then Professor Nakayama preferred to send a written format answers later on via email.

To avoid translation bias, all interviews were conducted in English. The square brackets represent the interview abstracts. The expert's initials are listed first, followed by a colon and then the line number of the quote.

The list of initials is as follows:

- SW: Steve Wheeler.
- AN: Akinori Nishihara.
- MN: Minoru Nakayama.
- PB: Peter Bryant.
- JR: Jekaterina Rogaten

Interviews with experts revealed the following main outcomes concerning the 11 open-ended questions:

- Relevance of the identified research problem, it is always considered a vital issue, and as e-learning and distance education researchers we are always facing this problem, so the solution should be valuable [AN: 7, 8]. Professor Nakayama also believes the problem surely exists and is the huge obstacle to spread e-testing, hence both tight invigilation and privacy of participants should be well considered, so the developed system may be a solution for the issues [MN: 10:13]. From extensive experience in the Open University delivering online assessments, Dr. Rogaten says it is the research problem that needs to be addressed [JR: 18] and little things have been done to have good invigilation systems for online assessments.

  However, Associate Professor Wheeler thinks it is interesting research problem but varies from department to department within different universities across the world, in some universities and in some departments and faculties within the university see the different problem, some see it as a severe threat, some see it as a mild threat, and others see it as not major problem at all. Therefore, it depends on the subject, the level of study and even the culture of the university. For example, in Plymouth University the variation will be between the different subjects, so in Education School, for instance, they do not have exams, then there is no problem in this regard, in Science School in the other hand, they have written exams periodically, the academic would feel it represents a problem. Thus if the university was a dual mode or even a distance university then it could be seen as a real threat [SW: 7 – 21]. Generally, cheating problems in Asian and American institutions are much bigger than in the UK institutions, the challenges are growing up particularly in the increasing online or distance-based examinations. Consequently having that capability to successfully conduct online exams is critical [PB: 13 – 19].

- Regarding the importance of utilising continuous and transparent authentication in e-invigilation of e-assessments, both Professor Nishihara and Professor Nakayama believe that it is essential and a critical process [AN: 13 – 15, 18, 19]. Additionally, any feedback information, whether participant acting well-ordered or suspicious behaviour, might improve their attitude [MN: 23, 24]. From a psychological perspective, Associate Professor Wheeler thinks that as far as academic so concern it would be a great process, however, from a psychological point of view, students might not feel very comfortable. For instance, some students might feel they are being monitored where not should be, some students who are paying high fees might worry about their privacy during such continuous monitoring [SW: 25 – 28]. It also depends on the scope of the exam, Mr Bryant, for example, says in open book exams the authentication, in this case, would not be implemented continuously during the test as suggested, but if there is a fixed time process – two- or three-hour exams – it is necessary [PB: 25 – 29]. While Dr. Rogaten thinks it has a potential to be implemented, she has one concern about the feasibility of conducting the e-assessment outside laboratory, for instance, poor Internet connections/networks at student home, which might represent extra pursue on the system and could affect the overall system performance [JR: 26 – 33].

- Concerning the feasibility, achievability, or practicality of the method. It is quite feasible [SW, 43; PB: 45] as long as the required technology is available [SW, 43], the face recognition version could be operated on a PC with built-in camera [MN: 28]. Additionally, it is more achievable and practical in an equipped laboratory inside the university [JR: 37, 38]. However, more details (more than the provided video) are needed in order to fully judge on the proposed method [AN: 32 – 34], the issue of student's psychological safety could affect the practicality [SW: 44, 45], how much the entire idea challenges the notion of trust between the institutions and the students, and in terms of distance-based learning, it would be expensive to get students equipped with this type of technology when usually they would use their own machines (e.g. iPads, MacBooks or any other laptop) [JR: 45 – 48].

- The proposed biometric modalities in the developed system are very transparent and robust, Associate Professor Wheeler and Mr Peter Bryant trust that the proposed biometric modalities are entirely robust, because it has already been implemented

[SW: 54, 55; PB: 75, 76], it is also considered very transparent and user-friendly [SW: 56; PB: 61,62]. In addition to its robustness and transparency, the method is collecting and storing data in very efficient and feasible manner – from her wide experience in the Big Data field – Dr Rogaten says: even if it has been scaled up to about thousands of students it could work sufficiently, furthermore, the whole idea of taking 2D, 3D, Eye Tracking, voice recognitions are all very good [JR: 53 – 58]. Nevertheless, some additional conditions should be confirmed such as various luminance level on the face, glass shape change, hat, scarf and make-ups, emphasising eyebrow, or lip shape, [MN: 34 35].

- Regarding the value of the security provided by the system it is accurate, for example in terms of HCI aspects, the used and tested methods (e.g. eye tracking and head movements) are efficient [SW: 60, 61] and all in all these types of systems can be quite secure [SW: 62]. The tested scenarios were perfect such as the phone pictures, swapping of the faces, putting a picture of another person on participant's face and many other activities. The idea of employing voice recognition was very creative and novel [JR: 73 -76]. Moreover, regarding the performance of accuracy that has been reported, all procedures are sufficient to use. Yet, the performance may depend on the condition of application such as e-testing and the environment [MN: 39 – 41]. It is always important to achieve this sort of security, however, the student privacy should also be taken into account [AN:49 – 49]

- To evaluate the security provided in terms of minimising the opportunities of cheating threats. With such system, Associate Professor Wheeler thinks that the people would not cheat or even try to cheat if they knew they are being surveyed, though having said that there is always the possibility of someone trying to cheat, however, the provided security and authentication methods are robust, and hence they are very difficult to be faked [SW: 67 72], it is incredibly comprehensive [PB: 90] and quite secure although a one hundred percent secure may not be possible [AN: 61, 62] therefore any types of feedback during the observation may be vital such as the status of indication for valid or suspicious. The information will give all participants a kind of trust for the system. Also, it prevents cheating [MN: 48 – 50]. Nonetheless, while Dr Rogaten believes it is quite robust and can minimise the obvious cheating, however, the only concern she had is whether the system can trace some sort of non-

obvious or small scale cheating, for instance where there is a piece of paper next to the examinee because he/she cannot remember certain dates or names, and that is literally a fraction of the second to get it [JR: 81 – 86].

- To ensure whether the robustness of the developed system enables it to completely replace the position of a physical/human invigilator or not, generally, everyone in the expert group has given different but positive opinion about this issue. Dr Rogaten agreed that the system is robust enough and can completely replace the position of a physical/human invigilator [JR: 91], Professor Nishihara also thinks there is a possibility to do this [AN: 67], and Mr Bryant implied that the system has this ability [PB: 107 – 112]. While Professor Nakayama thinks the replacement may be possible in the controlled conditions but the feasibility may depend on the overall testing situation. [MN: 55 – 58], and Associate Professor Wheeler agreed that the system has the potential to replace the position of a human inspector but not completely, but ultimately the invigilation process would be improved [SW: 83]. However, even though it seems secure enough, some academics might not agree on the complete replacement, therefore the next researcher job is how to change the mind-set of any instructor and persuade that the system is secure enough and human power can be saved [AN: 67 – 72]. Furthermore, Dr Rogaten raised a point, wondering if something goes wrong the test or with the system, you will still need to have a human to fix a problem? it may be not the person who watches the exam, but a person who mainly watches all the systems are running properly. The cost and benefit also need to be calculated to see if the replacement is feasible for both in laboratory and distance based examinations [JR: 90 – 106].

- Relevance to the robustness of the experimental validation of the approach, most experts agreed that the experiments have provided a very robust validation of the approach [SW: 88 – 90; MN: 63; PB: 117 – 120; JR: 111], however, Professor Nishihara did not fully understand the experiment details provided by the video, therefore, a published peer reviewed paper about this experiment has been sent to Professor Nishihara to provide more details that would enable him to make a clear comment [AN: 77 – 105] (another expert commented on that publication “the results look like an authentic publication which in peer reviewed journal with the good data” [SW: 89, 90]). The experimental design has been created to efficiently and logically

to evaluate the accuracy by considering both testing situations and participant's behaviour [MN: 63 – 64; PB: 120]. The accomplished experiment was very accurate it did show the system is working, however, a human double-check still needed [JR: 111 – 118].

- Moving forward to exploring the experts' opinion about the system's strengths and weaknesses, thus two lists of both can be driven from their opinions:

  Strengths: (in addition to several points already implied in their previous responses, all the academics indicated several strengths)

  1. The system could possibly replace the human invigilator [SW: 94, 95]. It is robust enough and can completely replace the position of a physical/human invigilator [JR: 91].
  2. It is clear that the system can save man power [AN: 109 – 110].
  3. It can assure robust and transparent authentication [AN: 110].
  4. "I agree with the strengths of developed system as you mentioned" [MN: 69]
  5. It makes the examination process open, and that is great [PB: 119].
  6. It increases the examination flexibility [PB: 120].
  7. It increases the capability of the institution to do flexible learning [PB: 121].
  8. In addition to the traditional security restrictions, the system utilises many efficient methods of preventing cheating such as 2D and 3D facial recognition, voice recognition, and eye tracking [JR: 123 – 127].

  However, the experts stated some weaknesses/remunerations/concerns that some of them are already achieved or taken into account, and others can be implemented in future systems.

  1. As long as it is an online process, there is always a possibility to be hacked [SW: 96, 97].
  2. "well I don't see particular weaknesses at this moment, but probably as I told you before some instructors may do not like to use such system if they do not believe the system that may be a problem." [AN: 111 – 113].
  3. "It may not a weakness; responses of participants who have joined the experiments should be considered. For example, if participants feel strong mental stress, it is not easy to introduce the system." [MN: 69 – 67].

4. A lot of people quite suspicious if their biometric data go out [PB: 118, 119].
5. The cost benefit analysis of the hardware installation would be the hardest part [JR: 128 – 130].
6. How friendly it is to people who have learning disabilities [JR: 131, 132].

- When it comes to identify the key barriers moving forward, Associate Professor Wheeler still insists that the key barrier is the psychological, "if you put students in a position where they feel threaten in some way, will they perform less ably than the way when they did not feel threaten?" [SW: 103 – 105]. Furthermore, the key barrier is data security including the cost involving the data security and the data collection particularly biometric data [PB: 125 – 127]. Therefore, it is important to show the users sufficient evidence in order to persuade them that the system is robust, transparent, and secure [AN: 118 – 120]. In addition to her concern about the system's expenses, Dr Rogaten also has another concern about how can the elderly people (who still represent a large portion of online learners) cope with such new technologies suggested in this system [JR: 136 – 143]. Furthermore, in general, if the system has been deployed in the market, then it might need some adaptations in response to the institution requirements [MN: 76 – 79].

- Finally, in general, all experts did not have anything more than what they have already mentioned in their previous answers. Nevertheless, some encouraging quotes have kindly been said including:

  - "It is an interesting area of development I wish you successful at it. [SW: 110, 111].
  - "I think it is an interesting project and it has some mileage to it" [JR: 147].
  - "I think it is really really fascinating" [JR: 150].

Despite the fact that majority of the experts' opinions were positive on the project via their answers to the asked questions, they had/raised, however, some concerns and recommendations that can be discussed including:

- Regarding a concern about the psychological safety of the student due to they would feel being monitored continuously, while there is no escape from student monitoring during taking the assessment whether it was electronic or any sort of traditional

assessment, this concern should also cover all proctoring processes and not restricted to e-assessment.

- Concerning the feasibility of conducting the e-assessment outside the laboratory and the poor Internet at student home, this rather generic problem and could not be considered a problem or a barrier for a particular system as the experiment results have proven the system feasibility in this regards. The entire e-learning process, in that case, is exposed to the same limitations.
- To achieve a secure e-invigilation, in general, the system is proposing the idea of utilising technologies that currently available and it is not a huge stretch in the imagination to think that in time there will be more advanced technologies available. As it has been discussed in Chapter 5, the main technologies (for implementing 3D facial recognition authentication and eye tracking security) are currently built-in most PCs and there is no doubt that the future applications will contain these abilities widely. Therefore, the expenses would be far less than the expectation of some experts.
- The system does not suggest any limitations over the normal and usual conditions, for instance, the luminance level on the face within the normal settings. Furthermore, There is no limitation on wearing any sort of glasses (During the experiment, many participants were wearing medical glasses – some of these glasses with dark lenses, however, this does not affect the eye tracking or the authentication processes as the infrared beams can penetrate any sort of lenses/glass perfectly). Some participants also took the exam wearing head veils, scarf, make-ups or hat; this however does not affect the recognition efficiency.
- Supposing a fraction of the second to be valuable to get useful cheating information would be over an ambitious idea. However, the eye tracker is always there to check whenever the eyes were outside the predefined coordination or not, that is the level of flexibility is an academic final decision.
- As discussed throughout the thesis, in addition to various problems that would come from relying on human invigilator, utilising the proposed approach still, by all means, cheaper than hiring human invigilator.
- Every online service (e.g. military, financial and banking information) is exposed to be hacked and the e-learning including e-assessment is not the exception, therefore securing this side is of course in mind even this is not the main focus of this research.

- Currently, many countries around the world are using the biometrics for human authentication and identification (e.g. airports or visas), furthermore, many institutions/technologies nowadays employing those data for security purposes (e.g. mobile and banking authentication). This growing trend would encourage people, more than any previous time, to give their biometric data to be used for securing e-assessment.
- Unfortunately, as with every other system (e.g. the traditional learning systems), the people who have learning disabilities need of course special and totally different examination procedures that can ultimately fit their needs.

7.3.2 Outcomes of the Academics' Group Interviews

For anonymity it was given a code for each academic name, the list of codes is as follows: A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A12, A13, and A14.

The square brackets represent the interview abstracts. The academics' initials are listed first, followed by a colon and then the line number of the quote.

Interviews with academics revealed the following main outcomes concerning the 9 open-ended questions:

- The system needs to be a user-centric through the application of HCI principles, which is one of the main e-invigilation system requirements. The format and layout of the interfaces are considered as easy to use, comfortable, convenient, simple, understandable, attractive, and sufficient. A set of 14 academics' positive viewpoints regarding this can be stated here:

- It is easy to use, comfortable, and can speed up the process of everything [A1: 12, 13].
- "It is convenient in use and very comfortable in practice" [A2: 5].
- "The format and the layout of the interfaces are well designed and the message was easily conveyed" [A3: 5, 6].
- "The format and layout of the interfaces provide one of the best and simplest page layout software. It offers an incredible number of tools and features that may seem overwhelming if you are new to page layout design software. For example, the software contains only five taps with important one for help. All settings, actions and tools are conveniently located, and the layout can be customised as you need. These

incredible features enable the user to easily and quickly learn how to use this software" [A4: 5 – 10].

- A5 thinks the layout attracts the user's attention on the points of interaction. The student's registration interface offers more than one method to log in. It also starts to convey how the system works to the user through the eye tribe calibration. The alarm manager also helps students to keep within the standard behaviour during their exams. The colour coded monitoring results in the invigilator interface can be easily interpreted thus minimising the teacher's task of looking for information in long reports or complex graphs [A5: 5 – 11].
- "The format and layout are simple and easy to use. It offers simple tools and features to use for new user. This is new page layout design software which is easy to set and learn to use" [A6: 5, 6].
- "The format and layout of the interfaces are very useful, understandable and clear. The features and tools that have been used are amazing, professional and perfect structure was built to this software. For example, if you are academic and not familiar with this software, it's easy way to find your choice out of five choices to go through it. All possibilities were included" [A7: 5, 9].
- "The layout of the interfaces is simple and easy to use and navigate through, which is one of the advantages of this system. The system is well designed to make life easier for both the academics and the students by providing them with a simple and easy to understand interface. I cannot see any difficulties to use the system by a simple user" [A8: 5 – 8].
- "It is easy and sufficient" [A9: 5].
- "It is excellent and provides simple and smart interfaces. The tabs and buttons are clear and useful" [A10: 5, 6].
- "They are simple and easy to use for both the instructors and the students; I can say one of the system's strengths is considering the principle of HCI perfectly" [A11: 5, 6].
- "I think it is good and everyone can deal with the system in easy way" [A12: 5].
- "The format and layout of the interfaces is well organised. It displays progression of activities to be performed step-by-step, making the system operationally usable with little or no additional help at all. In addition, the colours used are eye-friendly" [A13: 5 – 7].
- It is friendly to end user and very convenient in practice [A14: 5].

- Generally, the exam creation and manipulation have classified as efficient, simple and flexible processes [A1: 18 – 21; A2: 10, 11; A3: 11, 12; A4: 15 – 18; A5: 16, 17; A6: 11, 12; A7: 14 – 18; A8: 13 – 15; A9: 10 – 15; A10: 11, 12; A11: 11, 12; A12: 10, 11; A13: 12 – 14]. This is another excellent choice for page layout software [A4: 15], here, these interfaces play important role in speeding up the process of examinations [A1: 19 – 21; A6, 12; A7, 14, 15; A10, 12]. For example, to add a new test from the tests page just click on the (+) in the page button, and to edit test from the same page going to pen picture on the right [A7: 15 – 17]. The provided flexibility and accuracy [A2 11; A12, 10] would surely enhance the quality of examination procedures [A2: 10] and will minimise the opportunities of the occurrence of the errors [A1: 20]. They are well and clearly designed interfaces that are straightforward that they will take no time from the academic to learn how to use them [A13, 12; A8, 13, 14]. Hence, they are very usable, easy to understand [A13, 12, 13; A7, 14], simple, friendly and clean workspace with conveniently located menus [A4, 15, 16; A5 16, A6, 11] which enable them to perfectly handle the activities such as creating, viewing and editing exams [A3, 11,12; A4, 17,18; A5, 17; A11, 11]. Finally, the page colour schemes and icons are clear and simple which makes this page layout design software easy to use [A4, 16, 17, A6, 12].

  While the academic A7 considered inner exam creation as one of the interfaces advantages, the academics A9 and A13 do not think that there is a need to include the create option with the edit one [A9, 12, 13; A13, 13, 14]. Nevertheless, this was designed to increase the options for the academic to achieve the exam creation within the inner interface without the need for a backward step, the same procedure was used in both interfaces, so it was simply a process of recalling an already existing procedure.

- Moving forward to exploring the academics' opinion about the system ability to detect and judge cases of misuse, most of them to a great extent agreed that the academic interfaces allow the user to quickly, easily, and efficiently identify and judge cases of misuse [A1: 26 – 30; A2: 16; A3: 17; A4: 23, 24; A5: 22; A6: 17, 18; A7: 23, 24; A8: 20, 21; A9: 18; A10: 17, 18; A11: 17, 18; A12: 16; A13: 19, 20; A14: 16, 17]. Moreover, the system used robust strategies, security techniques and

biometric modalities that enable it to sufficiently achieving this [A1, 28 – 30; A2, 17, A4:23, A7:23, 24, A12:16, 17]

However, A5 and A9 have concerns about the strategy of identifying cases of misuse, "The software offers the user to verify true positives (when there is detected true cheating) and ignores false positives (when there is a false alarm). The only part that I am concern about is the false negatives (when there is an undetected cheating)" [A5: 24 – 26]. In the former quote the academic did not explain what sort of undetected cheating, which reduces the chance to discuss his concern in details, nevertheless, the previous chapter presented the results of the conducted experiment where the FRR and FAR were very satisfactory, therefore, the provided authentication approaches have been empirically proven it can confidently help to minimise the opportunities of cheating. [A9: 19 – 22] expected there is however a possibility of cheating via very small headphones inside the student's ears and make the computer screen available for someone else who can, in turn, help him in answering the questions. As discussed in similar scenarios (5, 6 and 7 – see section 6.2.2), the neighbouring illegitimate person should be very close to the examinee to do this, in this case, it will be impossible to avoid the camera that captures more than one face in both 2D and 3D modes. In addition, if another individual answered the questions orally, the JSGF algorithm captures every spoken sentence in both modes. And finally, it is extremely difficult to hold and handle both the camera and the eye tracker or mimic original locations. Therefore, the system will capture too many illegitimate photos via both eye tracker and 3D camera security subsystems. Nevertheless, moving the computer screen to another individual cannot be achieved in future due to the 3D camera itself will be built-in the computer.

To make the identification easier and faster, A13 suggested adding a summary of security/authentication problems with the overall grade for each course or a list of security/authentication problems for each course in the authentication results section [A13: 20 – 22]. The academic here thought there is a grade/score presentation, despite this misunderstanding, but this would be repetitive, as it already exists in the presentation of the authentication results.

- A subsequent question in this domain was asking the academics whether the system gives them the information they need or not, all the responses were very positive, both academic A2 and A14 answered with only one word "Yes" [A2: 22, A14: 22], others

gave short encouraging sentences expressing their opinion about the system's adequacy and sufficiency [A1: 35; A3: 22; A7: 29; A9: 27; A12: 22; A10: 23]. The rest comments were more comprehensive. This system provides:

1- "Sufficient details for individual authentication and security results whether there is a security problem in a particular period or not" [A4:29 – 31].
2- Details about the problem such as eye tracking, speech and no face images [A4:31 – 32; A6: 24, 25].
3- The academic can navigate to show all the results and listen to the entire record during the exam time comfortably [A4: 32, 33; A8: 26, 27; A11: 23, 24].
4- Alongside the exam security information [A5: 32], it provides the standard academic explanatory and comprehensive information needed about the test times and student activities [A5: 31; A13: 27, 28].
5- It also offers legal evidence in the cases of reported cheating [A5: 32].

- Four academics simply agreed completely without any detail that the system allows finding and identifying the individuals that they suspect might be cheating in a timely fashion [A1: 27; A3: 27; A10, 28; A14: 27]. However, the rest 11 academics provided more coherent and objective details. In this particular point, the system definitely works better than the current working commercial systems [A5, 37], and offers very effective and accurate approaches to access the students' information. Therefore, it can be recommended to handle such a large group (c. 200+) sufficiently [A1: 42, 43; A6, 30; A7: 35, 36; A8, 33; A11: 29, A7: 34 – 36], and this can be considered an important advantage of the developed system [A4: 38; A6, 31; A8: 34]. Furthermore, it can provide legal evidence [A4, 40, 41; A6: 32] by acting as an 'impartial witness' to allow the university/department managers to 'see both sides of the story' if a dispute arises [A4, 40, 41]. "It would also help safeguard against substitute candidates sitting exams on behalf of others, and stop students claiming their poor grades were due to errors made by those supervising the tests." [A4: 41, 43].

  To a certain extent each of [A5, 38 – 40], [A9, 32 -34], [A12, 27 – 29] and [A13, 33 – 35] agreed that the system would allow finding and identifying the students who might be cheating. A5 said the required supervision for each single alarm might be time-consuming with a large number of students. But the number of actions that can be considered as cases of misuse are far less than what A5 thought, this as a result of the predefined time limit policies that restrict the reports to certain and limited cases.

For example, about 1% of the eye tracking captured actions would be reported as cases of misuse. A9 thinks it can be better to enable the software to define the cheating and misuse cases and show them to the academic. However, the system does define and show these cheating and misuse cases to the academic, the academic merely needs to check the detected cases to either confirm or deny cheating, when the final decision should be taken. Both A12 and A13 worry about the consumed time by the academic staff that would spend a long time to check every student for the same issue. This opinion would come from the misunderstanding of specific details in the presentation video of the project; the system does not enforce the academic to "check every student for the same issue", it detects and reports only the suspicious actions.

- The system might be able to completely replace the position of a physical invigilator. Generally this idea got positive responses from the academics; the agreement varied from respondent to respondent, and most opinions were comprehensive, yet they can be divided into two groups:

  1- The academics who believe that the system can completely replace the position of the physical proctor including:

  - Academic [A2 32, 33] admitted that the system could act as human invigilator within all universities especially for the universities that carry out the electronic learning [A7 41, 42].
  - In very close positive response [A7 41, 42] believes that the robust features he had seen in the system can definitely enable this program to completely monitor students without any human instruction.
  - Furthermore, academic [A8, 39, 41] thinks the system is much better and more efficient than a human invigilator, to support this strong opinion he stated: "a camera will closely monitor every student and even his eyes movements will be monitored, and this cannot be done by an invigilator".
  - About 20 years of experience as a lecturer in the university, give A10 confidence to say: "using this system in the examination environment would open the door for the opportunity of replacing the human completely" [A10, 33, 35].
  - A11's answer shows absolute agreement, the system's robust authentication and active multilevel of security encourage him to state that the future is

indeed for this kind of system, and definitely able to completely replace the position of a human invigilator [A11: 35, 37].

- From his experience as an invigilator for two years in the University, A5 thinks that the human monitoring systems are not perfect. A large number of students participating in one time could maximise the problem and might encourage some students to cheat. This system can strongly support the human system if it is combined with it. It also looks valid enough to replace it after adequate testing to avoid any technical problems [A5: 45 – 49].
- The trendy efforts are going toward using the technology instead of human beings, therefore, it will be very feasible [A14: 32, 33].

2- The academics who stated explicitly or implicitly that the system can partially replace the position of the physical proctor including:

- "Having a camera watches the candidate, and software keeps monitor him gives greater latitude for the institution to adjust the timing of exams to whenever and wherever they want without having a human invigilator to monitor students. In other words, if a student's eyes start to wander, the developed system gives a warning signal, just as a human invigilator might tell students to keep their eyes on their own papers. By doing this, students will be given a great option for participating at local testing centres without traveling to regional testing centres at exam time, and reaching such centres which is difficult or impossible for many students. It is the same for working adults who can't take time off to travel or others in far-flung places who can't afford the trip. However, the presence of a human invigilator is essential for students because the human contact influences them in positive ways. Firstly, students realize that they are not dealing with a machine but with a human being who deserves attention and respect. They also learn the importance of relying on themselves, which helps them improve their social skills" [A4: 48 – 60].
- The problem is different from country to country, in developed countries with the modern universities; the system could be applied perfectly. But with the developing countries, for example, a country from the Middle East, where obviously there is a shortage in the required infrastructures, it is not expected to implement such system completely until filling the existing technical gap.

However, with small e-learning centres this system can be implemented completely [A1: 51 57].

- "It might replace human activity, but physical control is also necessary" [A3: 32].
- This approach could improve the academic examination and consequently reduce the number of human invigilators [A6: 39, 40].
- To a high degree the system can replace the position of the inspector during the exam time, but not completely [A9: 39].
- The system will help reduce the number of human invigilators and detect certain cases of cheating which they could not be identified, yet the existence of physical proctor still important [A12: 34, 37].
- In a very similar to the previous comment, A13 said the system would enhance the monitoring process by reducing the number of academic staff allocated to invigilate an examination, but not completely [A13: 40, 41].

- When it comes to gather academics' suggestions to gain any idea that might be helpful in system integration, five academics thought everything is fine or perfect, so they had not proposed anything [A3: 36; A7: 46; A10: 39; A11: 41; A14: 37]. Academic A9 had no suggestions more than what he already mentioned in his previous answers [A9: 43]. However, some suggestions can be driven from the other eight participants. While A1 was amazed by the system's interfaces, icons, and fonts, but he thinks the colours need some enhancements [A1: 67, 68]. A2 also said it would be good to enable the users to change the colours and themes according to their desire [A2: 37, 38]. With certain threats, such as internal defects or when the system breaks down, it would be useful to consider providing an alternative solution or warning signal to inform the academic [A4: 64, 64, A6: 45, 46]. As long as the system provides the results in a numeric form, it will be useful if graphical representations are provided [A5: 53, 54].

  Furthermore, A12 commented, "It is important to add some movement's features that acceptable by the system, because the student is a human not robot." [A12: 41, 42]. Despite the ambiguity of this comment, there is no limitation on any user's movement. And [A13: 46, 47, 48] suggests ensuring all fields are made compulsory when the academic is filling 'create new test' fields. But the system already does this.

  List of suggestions have been offered by [A8, 46 – 54]:

- The specifications of the used camera need to be discussed, to enable the system to accept a wide range of cameras to increase the system applicability in real life.
- To make the system more acceptable to a wide range of schools/institutes, low computer specifications need to be identified.
- Considering the required training in order to use the system by both academics and students.
- Adding a demo video for academics and another one for students to help and encourage them to use the system. (The same idea was suggested by [A13: 45, 46]).

- Comparing to the previous answers, the following responses (question eight) were the most coherent, comprehensive and rational commentary. Two lists of both system's strengths and weaknesses can be driven from the academic participants' opinions:
  Strengths: (All the academics indicated several strengths)
  1. The research problem is evolutionary, very novel and applicable with modern universities [A1 77, 78; A11, 46].
  2. The system offers very transparent, robust, safe, efficient continuous authentication and security, convenient and novel [A1: 79 – 82; A2: 44, 45; A5: 59, 60; A6: 51, 52; A7: 54; A10: 47, 48; A11, 47; A12: 47].
  3. The system data management was sufficient [A1: 83, 84; A2: 46, A9: 48].
  4. The system is very easy-to-use and user-friendly for both academic and student [A1: 85 – 88; A2: 47; A5: 60, 61; A6: 51, A7: 53; A9: 48; A10: 49; A13: 53].
  5. The system is determining the principle of HCI [A1: 90].
  6. The system controls large numbers of examinees [A3: 41, 42].
  7. Students would behave as self-dependent as they are aware that everything is rigorously controlled and no way for cheating [A3: 42, 43].
  8. The teacher would have the opportunity to be safe in terms of not interacting directly with the examinees [A3: 43, 44].
  9. The developed system would have an extra check on what was going on, in addition to walking past student's desks so a learning institution would be able to review recordings after the event to pick up on any inappropriate behaviour [A4: 71, 72, 73].

10. It could be used in examination halls to catch cheating and prevent unfounded complaints against invigilators [A4: 74, 75].
11. It would be useful to protect the rights of both the students and staff [A4: 76].
12. All data can be stored on a single server [A4: 77].
13. Eliminates human error in monitoring [A4: 78].
14. It can provide legal evidence and allow us to 'see both sides of the story' if a dispute arises [A4: 79, 80].
15. It provides detailed and comprehensive information [A5: 60, A6, 53].
16. It minimises the efforts in the examination process [A7: 55].
17. The structure of the system is very professional [A7: 56; A8: 59].
18. Technically, the whole mechanisms to prevent cheating (i.e. eye tracking, head movement, speech recording and recognition) are achieved [A7: 57, 58].
19. It is a great way to help academics and to make the distance and online learning more acceptable and accredited [A8: 59, 60].
20. It is a promising system trying to solve an actual and daily problem in distant-based learning [A10: 46; A11: 48].
21. Applicable to be implemented globally [A12: 47, 48].
22. The developed system is even better than human invigilator [A14: 42].
23. System independency from the external influences [A14: 43].
24. System results can be presented easily [A14: 45].

However, only six academics stated some weaknesses, recommendations, or concerns that some of them are already achieved or taken into account, and others can be implemented in future systems:

1. The technology is not always reliable particularly, so the information can be lost if a system breaks down [A4: 83, 84; A6: 56]. Consequently, the backup and recovery strategy is essential [A8: 62]. Actually, this important point, however, it is not this system responsibility to fix this, as long as the collected data (by the system) is feasible and reliable to be stored on a secondary storage medium. There is no doubt that any sensitive data should be saved securely and recovered whenever is needed, and this institutional rather than system level responsibility.
2. The costs to set up an e-assessment system might be expensive particularly for large groups [A4: 87, 88]. However, in the current system, both the 3D scanning and the eye tracking can be achieved utilising the same 3D camera.

Furthermore, with the currently released built-in 3D camera, more usability, reliability, applicability, cost effectiveness, and security are achieved. Hence, this is very feasible especially with large groups.

3. [A4: 85, 86] said the students might be worried about human rights, moral values and personal privacy.
4. In his comment [A5: 61 – 63] gave the reason as well, "The only weakness point is that it does not give a decisive conclusive diagnosis without supervision. However, it is an actual critical zone that has to be supervised anyway".
5. [A13: 53, 54, 55] said that the pages do not flow into each other. But the system interfaces are divided into multi-tabs in front of the user.
6. A9 has a concern about the registration process, he thought students should attend the physically in order to deliver their biometrics [A9: 48, 52], whereas this can be achieved even remotely. His concern would come from misunderstanding the system registration mechanism.

- Most academics did not have anything more than what they have already mentioned in their previous answers [A1: 94; A2:51; A5: 66; A6: 60; A7: 64; A9: 56; A14: 49; A11: 52; A12: 51; A13: 59].

  Nevertheless, some academics kindly congratulated the researcher for developing the system:

  - "You have done a great job, I really like the system and I cannot wait to see it applied in many schools and institutions. Good luck" [A8: 67, 68].
  - "I wish the researcher all the best to develop such incredible system completely" [A10: 52].

  And finally, from their career experiences as university lecturers, [A3: 49, 50] and [A4: 93 – 96] felt enthusiastic for applying this system in their countries for diminishing the common phenomenon of cheating in online examinations.

7.3.3 Outcomes of the Students' Group Interviews

In the following 15 quantitative questions, the combining of the responses of ranking 4 and 5(Most) will be considered as the majority while the responses of ranking 1(Least) and 2 will be considered as the minority.

The questionnaire starts with analysing the extent of students' opinions on the system log in process. Unsurprisingly, as can be inferred from Figure 7.1, it is similar to what is claimed by the researcher, more than 84% of the respondents considered the system log in process as a highly non-intrusive mechanism, the security comes in the second position with about 81%. Furthermore, more than 79% of the students feel the process is easy to use and convenient, and the majority of them (about 68%) did not worry about their sensitive data with this approach.

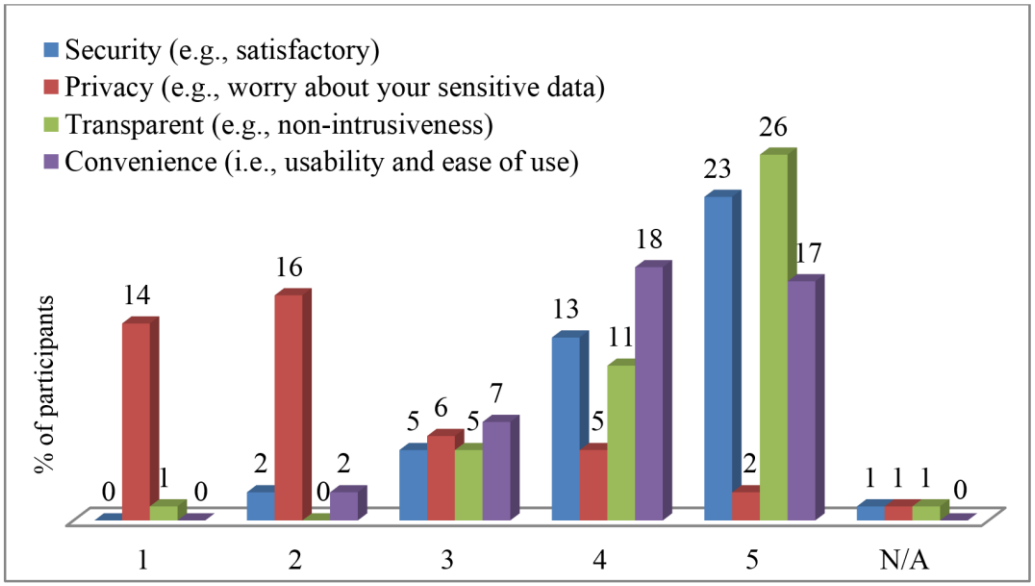


Figure 7.1: Analysing the Extent of Students' Opinions on the System Login Process

Figure 7.2 demonstrates that the format and interfaces were good enough to make about 79% of the students felt they were designed properly. Moreover, a larger percentage (almost 82%) goes to consider the system was very understandable. About two-thirds of the respondents agreed it is easy to use, but less than 7% of them were on the negative side. However, barely half of them satisfied with the system colours.

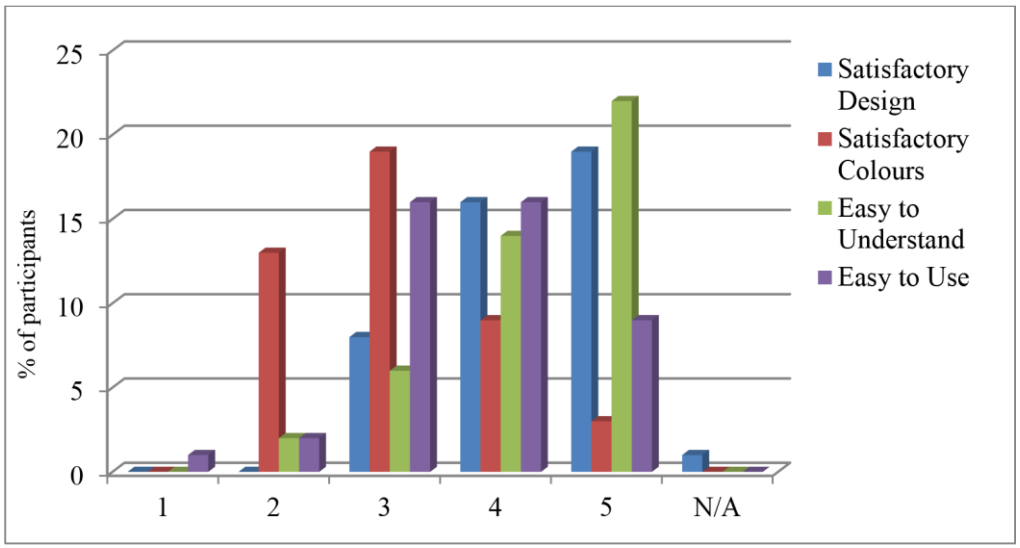


Figure 7.2: Analysing the Feeling of Students' about the System Format and Interfaces

When it comes to evaluate the ability of the system to detect cheating, to be applied over the Internet, to take the position of the physical invigilator, and able to be applied on a range of devices (e.g. Mobile), the findings in Figure 7.3 shows that over 79% of the students group believe that the system could detect cheating utilising the employed biometric modalities. Student perspectives/percentage regarding the applicability of the system over the Internet was slightly less than the former percentage (i.e. 18% selected '5', 38% selected '4' and 34% selected '3'). However, the majority of the participants (64%) felt that the system could take the position of the human inspector. Most of them (55%) also thought the system is able to be used on a range of devices (e.g. Mobile). Furthermore, 32% of them can be considered in the middle of the scale by choosing the rank of '3'.

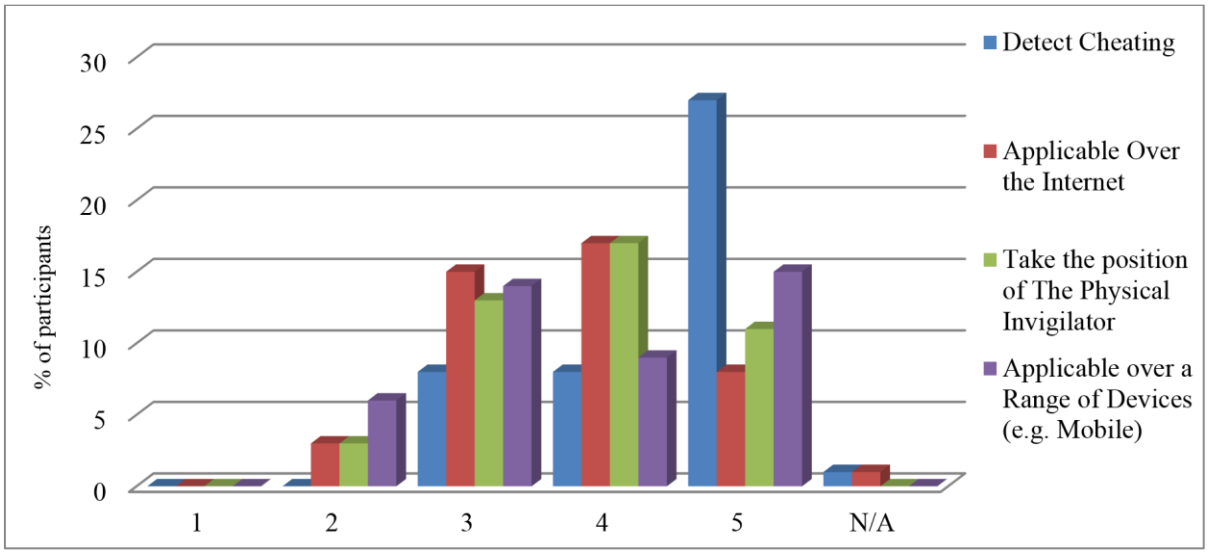


Figure 7.3: The Ability of the System to Detect Cheating, Applicable over the Internet, Replace the Position of the Physical Invigilator, and Applicable on a Range of Devices.

To evaluate the robustness and convenience of the biometric monitoring that are used in the proposed approach, Figure 7.4 depicts that it is similar to the responses of other stakeholder groups (i.e. Experts and Academics), students had either preferred to choose (‘4’) or more preferred to choose (‘5’), that is 86% of them believe the biometric modalities were very robust. And also the usability and ease of use of those modalities were either the preferable (‘4’) or more preferable (‘5’) to 84% of students. From this, it can be said that the biometric monitoring process has been considered as very robust and convenient.

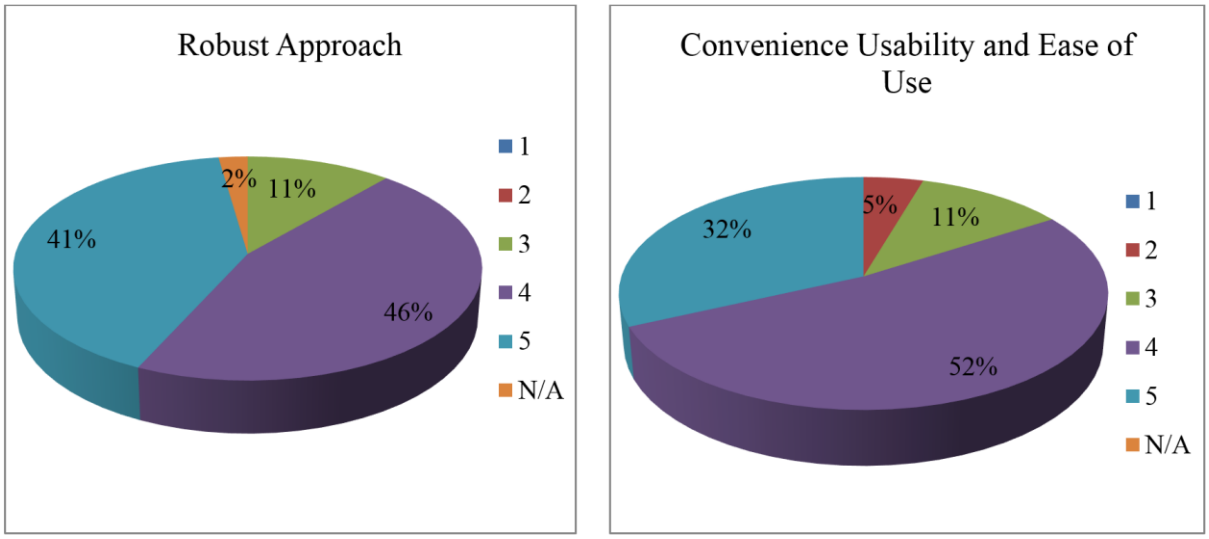


Figure 7.4: Robustness and Convenience of the Biometric Monitoring

Regarding the robustness and convenience of the security methods used in the proposed approach, Figure 7.5 illustrates that it is similar to the experts and academics opinions, students were either preferred to choose (‘4’) or more preferred to choose (‘5’), that is 84% of them believe the security methods were very robust. And also the usability and ease of use of those methods were either the preferable (‘4’) or more preferable (‘5’) to 80% of students. Having said this, it is evident that the security methods have been considered as very robust and convenient.

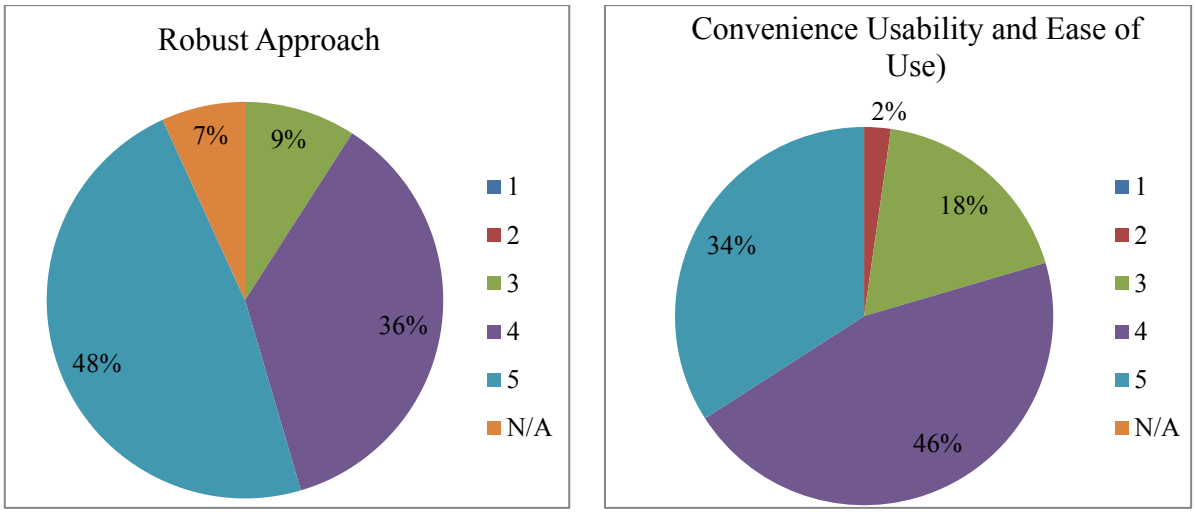


Figure 7.5: Robustness and Convenience of the Security Methods

Four consequence questions (6, 7, 8 and 9) were asked to investigate students' perspectives regarding many aspects including comfortability, privacy, immunity against spoofing actions, and effectiveness to be utilised for continuous authentication purposes of specific biometric authentication approaches including: 2D Facial Recognition, 3D Facial Recognition, Mouse Dynamic Analysis, Keystroke (keyboard) Analysis, Eye Movements, Head Movements, Linguistic Analysis, Iris Recognition, Fingerprint Recognition, Retina Recognition. Figure 7.6 presents that each of 2D Facial Recognition (91%), 3D Facial Recognition (84%), Mouse Dynamic Analysis (82%), Keystroke (keyboard) Analysis (79%), Eye Movements (82%), Head Movements (77%), and Linguistic Analysis (45% were chosen '4' and '5', but more than 43% were in the middle by selecting '3') were the methods that all students felt most comfortable with; this perhaps due to the high level of non-intrusiveness provided by each of these methods. On the other hand, each of Iris Recognition (48%), Fingerprint Recognition (48%), and Retina Recognition (41%), all students saw these methods less comfortable; this perhaps because of the low level of non-intrusiveness and/or sensitiveness of these methods.

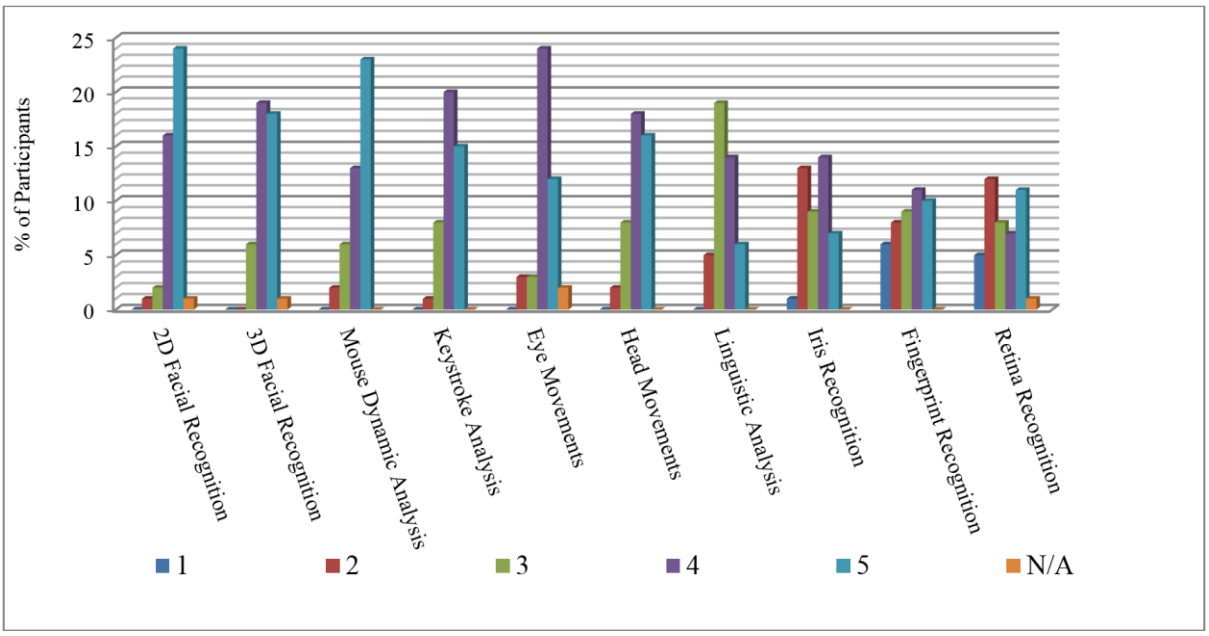


Figure 7.6: Students' Perspectives Regarding Comfortability

When it comes to student's privacy, in contrast to previous answers, Figure 7.7 demonstrates that each of 2D Facial Recognition (68%), 3D Facial Recognition (79%), Mouse Dynamic Analysis (75%), Keystroke Analysis (71%), Eye Movements (77%), Head Movements (75%), and Linguistic Analysis (40% were chosen '2' and '1', but about 48% were in the middle by selecting '3') were the modalities that most students found them as less threaten to their privacy; this might be due to many factors including but not limited to: the popularity, transparency, flexibility and robustness of each of those methods. On the other hand, each of Iris Recognition (46%), Fingerprint Recognition (37%), and Retina Recognition (34%) were the modalities that most students found them as more threatening to their privacy; this might be also due to the low level of non-intrusiveness and/or sensitiveness of these methods. However, in the responses of this particular question, the selection of '3' (middle) was relatively high in all categories.

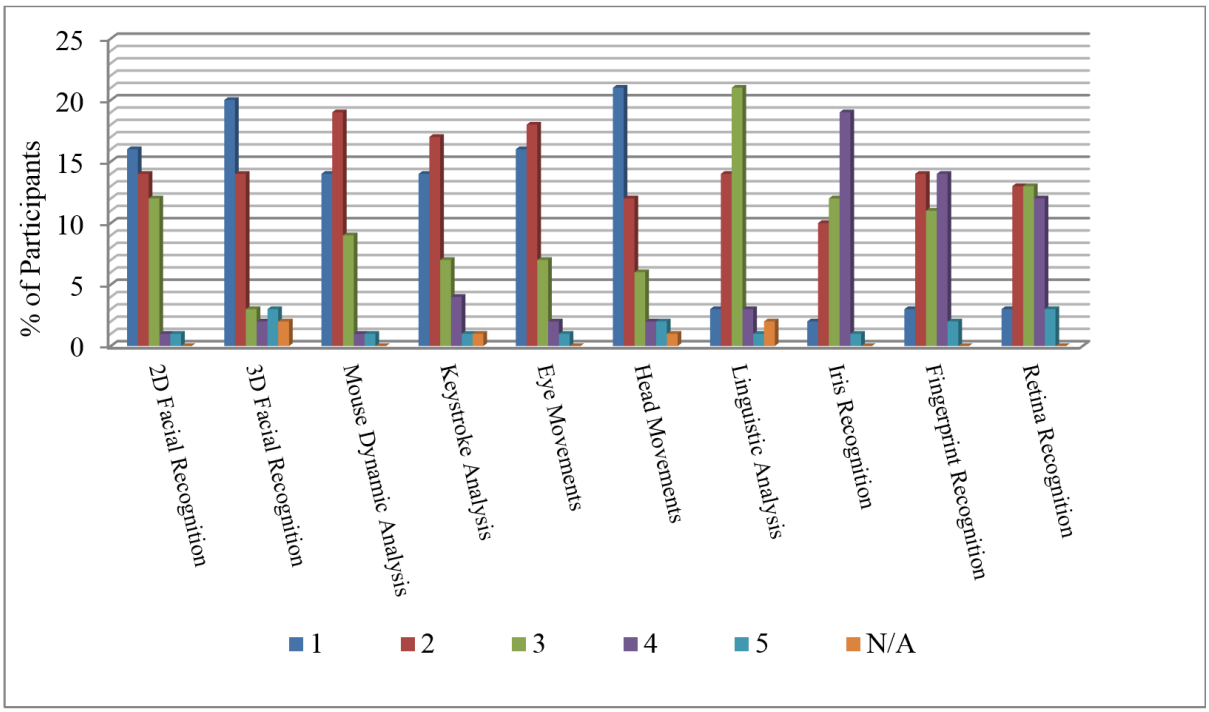


Figure 7.7: Students' Perspectives Regarding Privacy

Furthermore, when considering students' concerns about the proposed modalities immunity against spoofing, no surprise, as can be inferred from Figure 7.8, the 2D Facial Recognition and Fingerprint Recognition were the highest chosen modalities to be considered providing less immunity against spoofing actions, with 64% and 65% respectively. But Linguistic Analysis was considered moderate as most of the respondents have selected '3', where 63% of them felt it would be more reliable than 2D Facial and Fingerprint Recognition. The ranking of the rest modalities were considered very close to each other and have more immunity against spoofing actions than the previous three: 3D Facial Recognition (78%), Mouse Dynamic Analysis (75%), Keystroke Analysis (77%), Eye Movements (83%), Head Movements (76%), Iris Recognition (71%), and Retina Recognition (80%).

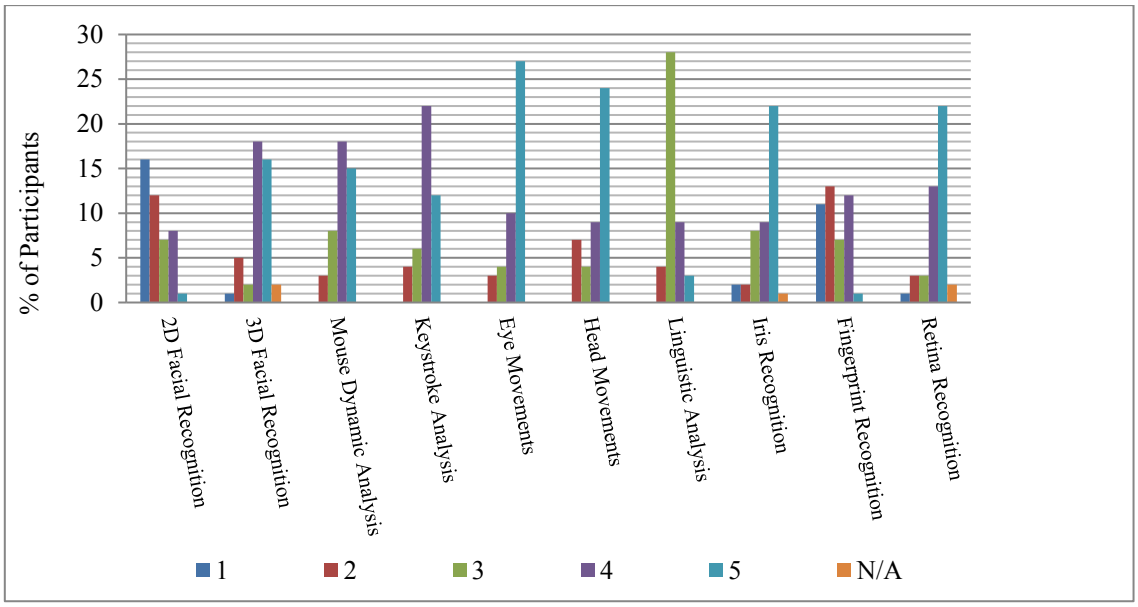


Figure 7.8: Students' Concerns about the Proposed Modalities Immunity against Spoofing

A subsequent question in this domain was about the respondents' point of view regarding the use of these biometric authentication approaches for continuous authentication purposes. Figure 7.9 demonstrates that each of 2D Facial Recognition (84%), 3D Facial Recognition (77%), Mouse Dynamic Analysis (75%), Keystroke Analysis (77%), Eye Movements (83%), and Head Movements (76%), were considered very effective modalities for that purpose. Linguistic Analysis also was considered moderate method as most of the respondents (about 53%) have selected '3', however, there was 25% went to '4'. On the other hand, each of Iris Recognition (57%), Fingerprint Recognition (53%), and Retina Recognition (50%) were not considered very effective modalities for that continuous authentication. Moreover, in the responses of this particular question, the selection of '3' was quite high for the last three modalities.

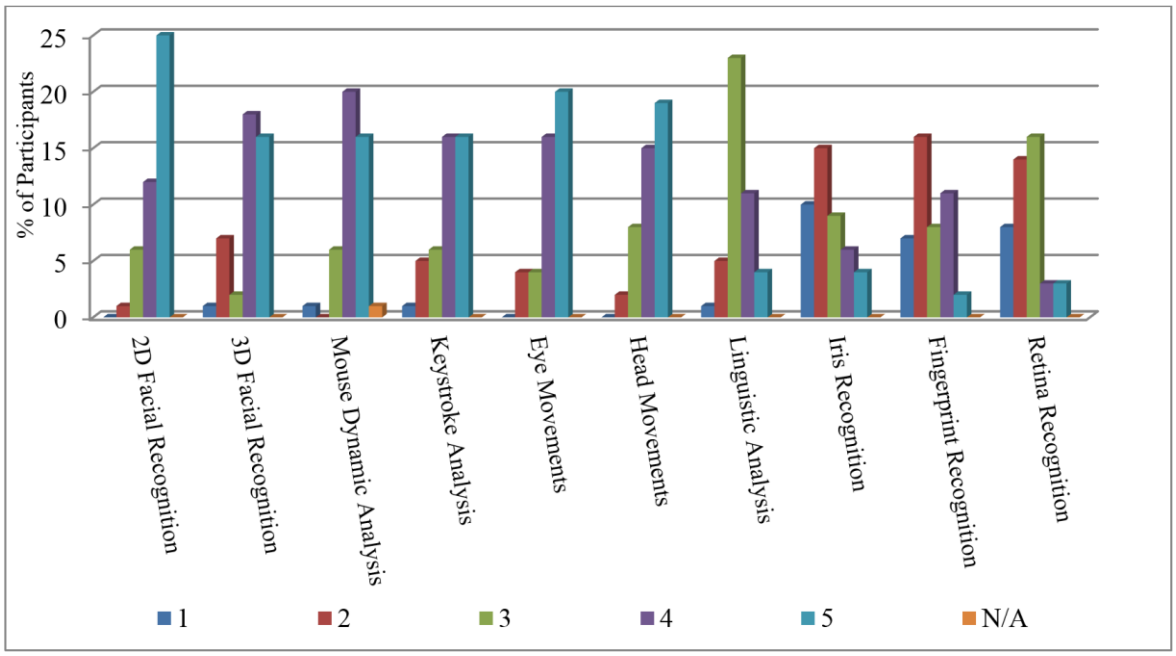


Figure 7.9: Respondents' Point of View Regarding the Use of Biometric Authentication Approaches for Continuous Authentication Purposes

A specific question was asked to investigate student's feeling regarding recording all the surrounding sounds during the test for security purposes, Figure 7.10 depicts that 35 of the 44 participants feel it is a safe and harmless process. About one-third of the respondents did not worry about their sensitive data, however, more than half of them selected the middle rank '3'. The process non-intrusiveness was rated as the highest feature, achieving about 80% of surveyed students rated it very transparent ('4'), or fully transparent ('5'). It can also be inferred that more than 82% of surveyed students considered it as easy to use.

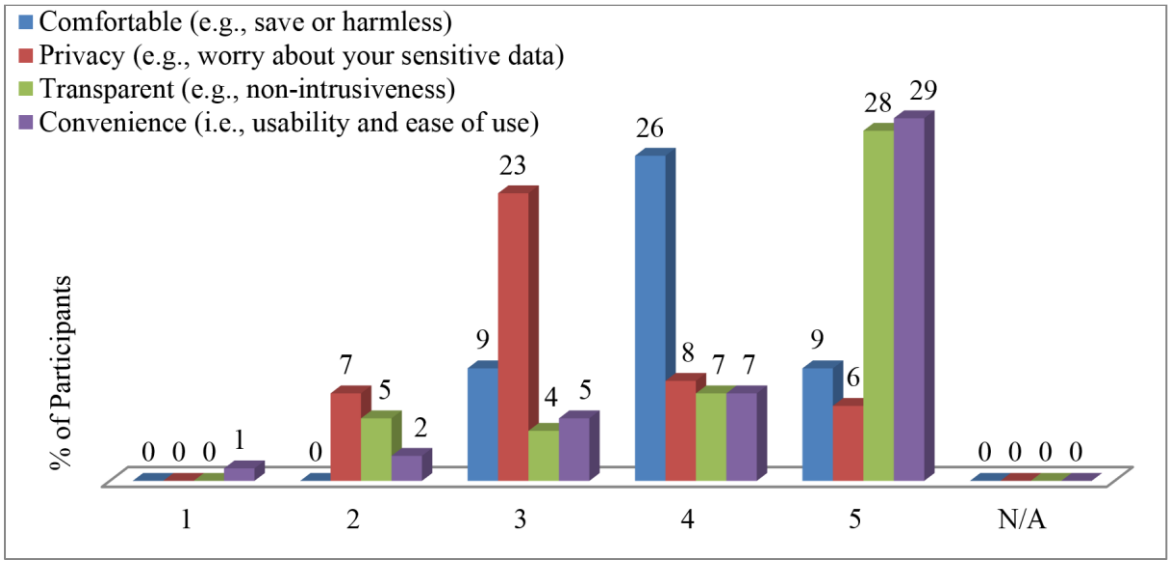


Figure 7.10: Student's Feeling Regarding Recording All the Surrounding Sounds during the Test for Security Purposes

Another question was asked to understand the student's feeling concerning employing the cameras/sensors with infrared lights in exam monitoring. As can be inferred from Figure 7.11, it is obvious that the vast majority of surveyed students think it is comfortable (80%) and convenient (76%). They also think it is essential (78%) and more secure process (84%). These results would strongly support the research viewpoint regarding employing the latest cameras/sensors with infrared lights in exam monitoring.

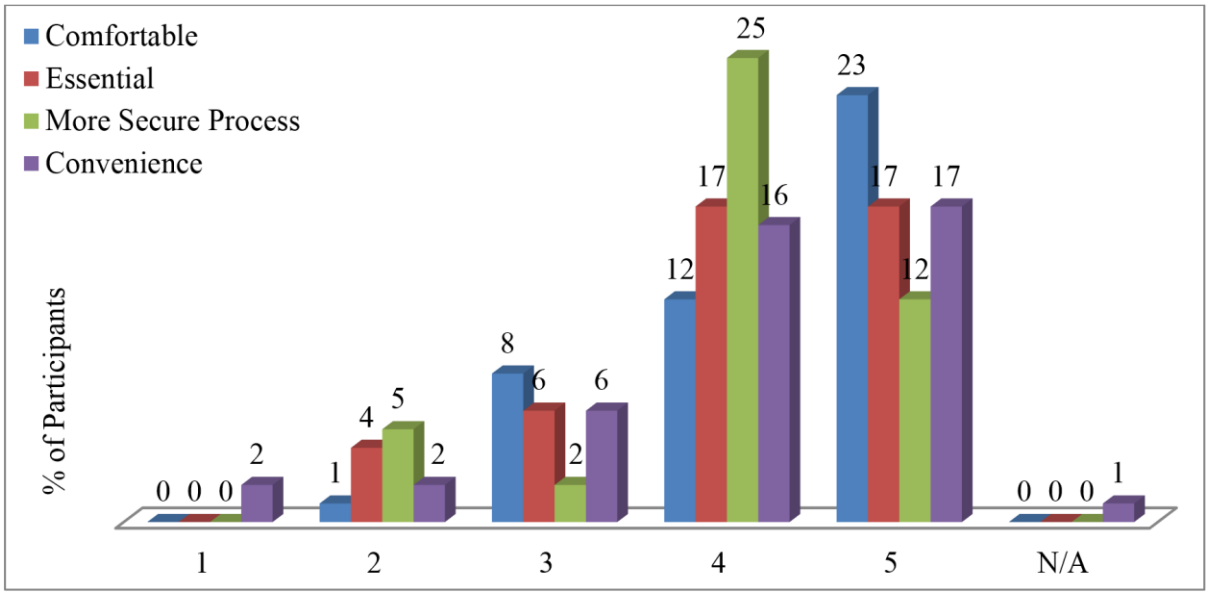


Figure 7.11: Student's Feeling Concerning Employing the Cameras/Sensors with Infrared Lights in Exam Monitoring

Furthermore, a subsequent question in the same domain was asked to understand how the student is thinking about involving the new technologies that enhance the monitoring process. Despite the fact that about only half of them felt it is feasible, Figure 7.12 illustrates that they are feeling comfortable (89%) and convenient (80%) with utilising these new technologies. They also think it is essential (80%) and would robustly enhance the online exam security (71%). These results would also strongly support the study viewpoint concerning proposing the latest technologies.

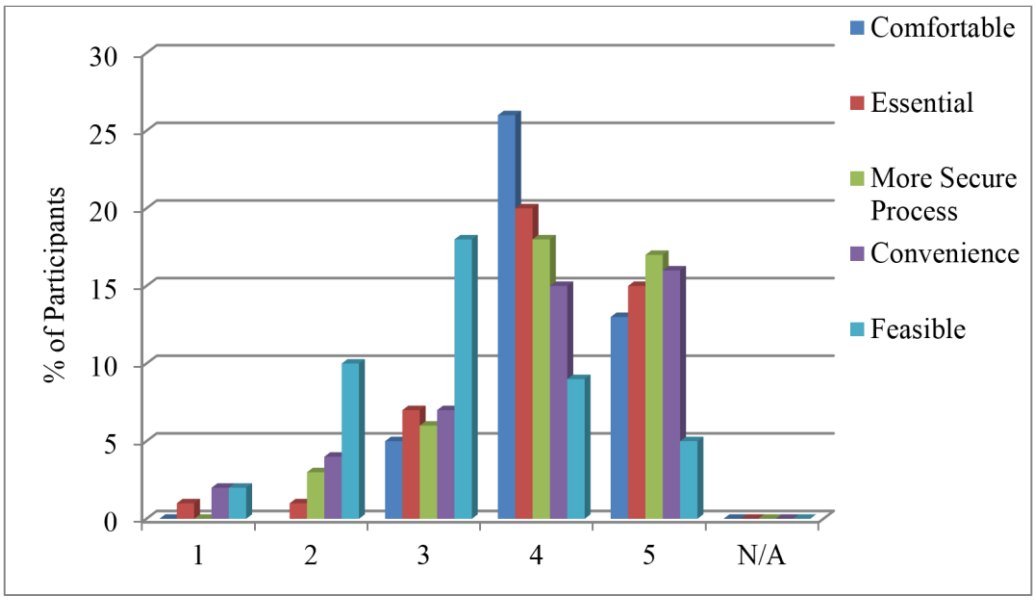


Figure 7.12: Student's Feeling About Involving the New Technologies That Enhance the Monitoring Process

To get a general idea about the students' thoughts behind the idea of having monitoring, as anyone would expect, while Figure 7.13 shows that only 35% feel comfortable, about 46% of the surveyed students are not. But 80% of them still think it is an essential process in order to control/detect/prevent cheating during the exam. The current/traditional available monitoring methods are not secure enough, where the majority of the students considered they are not secure but relatively suitable.

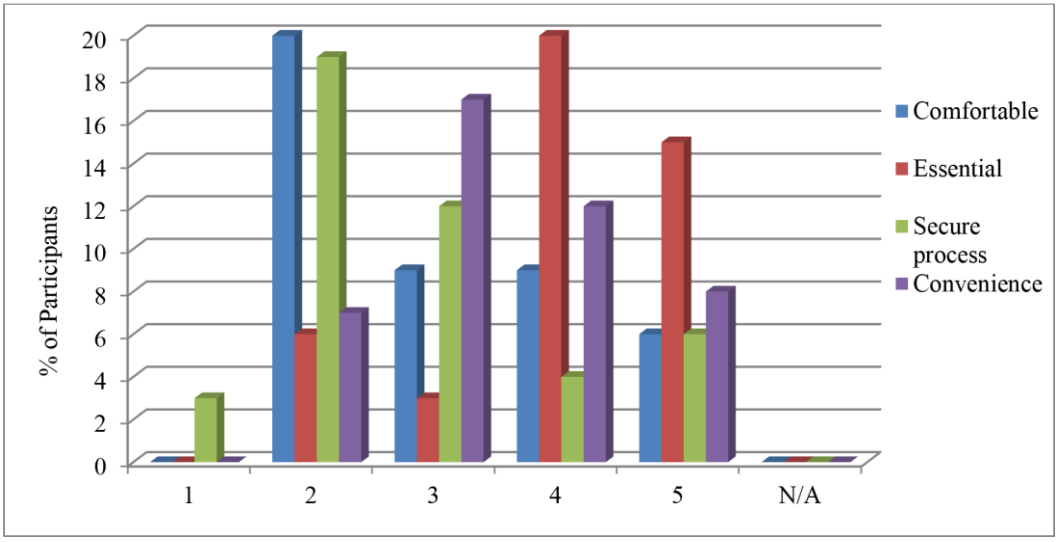


Figure 7.13: The Students' Thoughts behind the Idea of Having Monitoring

In comparison to traditional invigilation, Figure 7.14 demonstrated that the vast majority of the students prefer the e-invigilation over the traditional invigilation, where about 80% of the participated students felt it is more comfortable, and 82% believed it is essential and more

secure. However, there is no clear preference of either methods in terms of usability and ease of use.

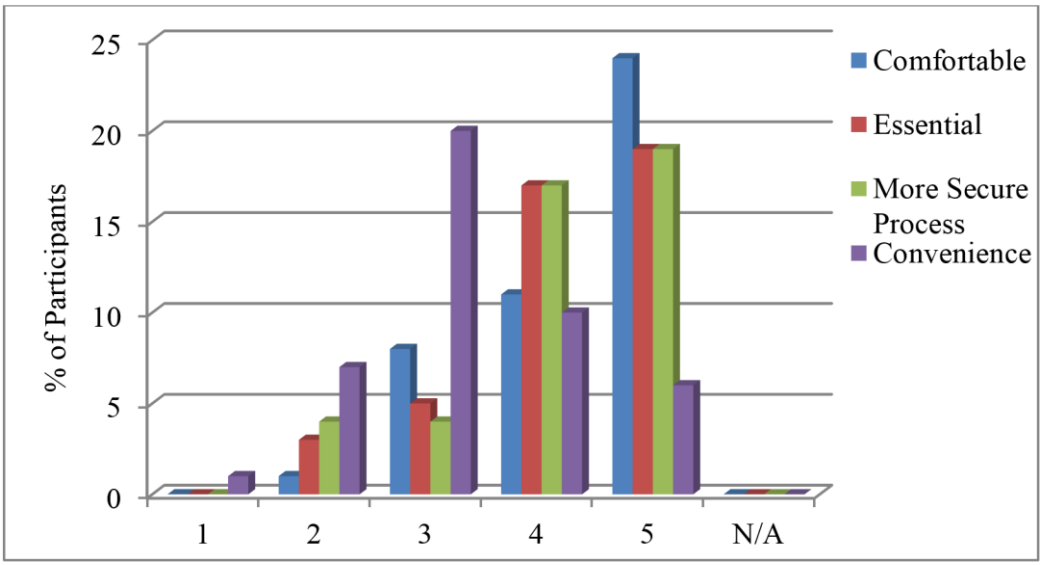


Figure 7.14: The Students' Thoughts about Traditional Invigilation

In these students' quantitative question list, the last question was asked to get the student's opinion regarding a complete room checking that would be done by most commercial proctoring systems. In terms of comfortability, Figure 7.15 inferred that most involved students (68%) would not be comfortable with this process. Two-thirds of them said it is not essential; most of them do not think it is necessary to improve the security, and only half of them feel it is easy and convenient to be done. Generally, these particular findings indicate that the student considered these methods as intrusive and impropriate, which support the suggested idea of transparent authentication.

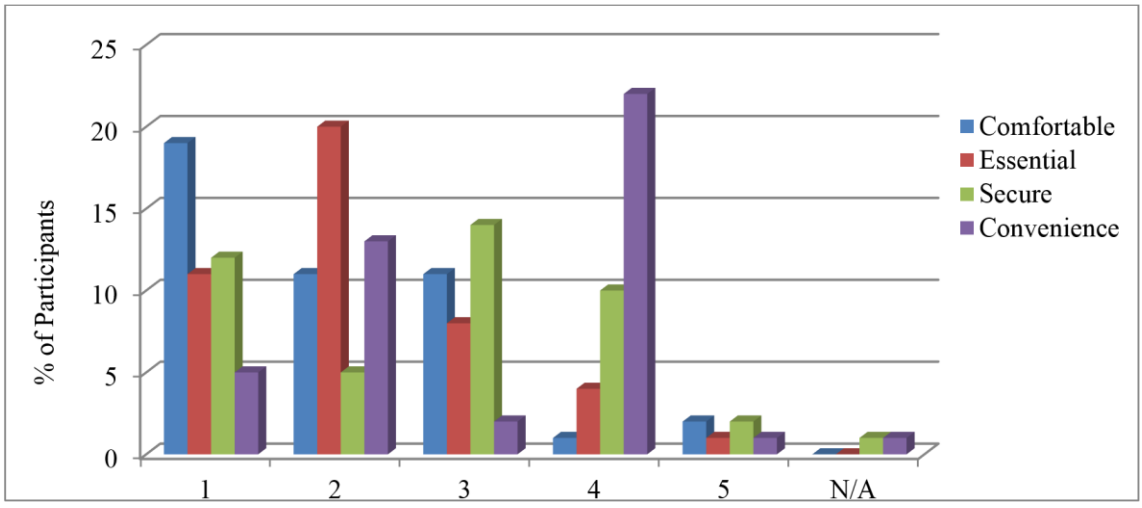


Figure 7.15: Student's Opinion Regarding a Complete Room Checking That Would Be Done by Most Commercial Proctoring Systems

Finally, as with the previous two groups (Experts and Academics), to give the respondents an opportunity to express their opinions, ideas or suggestions about the developed project or the entire research and every proposed idea behind it, the questionnaires ends with the closing question: "Is there anything else you would like to add?". However, only 10 of the 44 participated students have expressed their opinion using short but mostly positive sentences. Thereby, a set of 16 students' positive viewpoints/sentences can be stated here: (at the end of the Students' group question list – electronic Appendix C)

- Very good idea and can solve the problem of cheating among students.
- It is an important system as the security and authentication are strong.
- I considered it a successful approach to control the exams, and I suggest implementing it globally.
- I enjoyed the good interfaces of the student subsystem. I suggest enhancing the colours.
- The system has been designed professionally. I hope to apply it in all examinations.
- It is a good project, but difficult to be implemented it in countries that suffer from a lack in the Internet and computer devices.
- Very important idea, it is designed very well, but it needs to consider the wireless communications fraud cases.
- It controls all the cheating cases.
- Provides good interfaces. However, it needs to involve additional hardware, devices like fingerprint reader which would be expensive.
- It provides a good control and monitors the student efficiently. I suggest applying it to all universities.
- I really admire this project, the fact that it greatly reduces cases of fraud among students and the use of technology in exams will reduce the efforts of the teachers, as well as students, get their fair scores.
- I would like to apply this project in all the online tests.
- This project is essential in nowadays online examinations, from my experience with many assessments over the Internet (for example IC3 in my university), I can say there are many cheating actions happen in every exam, therefore these types of monitoring can play an important role to restrict cheating attempts.
- It is a strong monitoring system.
- It is an important research provides multiple monitoring methods.

- Well-developed system but expensive (tools and equipment), can be applied only in developed countries.

7.4 Conclusion

This chapter has presented a stakeholder evaluation by the three separate groups of stakeholders. The evaluation results have supported that the system has a large potential to be implemented for monitoring and eventually securing e-assessment as the identified research problem represents a critical issue needs to be tackled. The outcomes show that currently, with the rapid technological progress, the key barriers have become far less than a few years ago, as such security system is able to be applied over the Internet and on a range of devices other than PC (e.g. Mobile). Involving the up-to-date technologies is necessary to enhance the monitoring process as well as preserve the privacy and comfortability. The feedbacks of respondents totally agreed with the idea of continuous authentication in e-assessments as it is vital for ensuring solid security beyond the point-of-entry. From the stakeholders' perspective, the achieved transparent biometric authentication is also crucial and hence supports an essential principle of convenient and user-friendly monitoring proposed by the system. The results confirm that the security restrictions provided by the system are able to minimise the opportunities of cheating threats, this means the system is capable not just to detect but also to prevent the potential cheating. Hence, the experimental validation of the approach offers adequate and precise scientific evidence of a secure proposal as specified by the respondents. The outcomes have also proven the feasibility and practicality of the system, as it is imperative to suggest achievable approaches rather than proposing unrealistic and unpractical systems, such as involving further hardware devices or manufacturing a complete robot that merely provides monitoring. An efficient management of the system via well-designed, smart and attractive interfaces is one of the important achievements of the system that have been supported by the survey results, and have not been considered previously by other studies in this area, this will contribute to maximise the acceptability of the system, and hence increase its opportunities to be deployed widely. Ultimately, from the above discussion and as confirmed by many responses throughout the surveys, the system has the likelihood to fully replace the position of a human invigilator.

8 Conclusions and Future Work

This chapter highlights and concludes the main achievement of this programme of research. It starts with summarising the achievements of the research programme, then proceeds to discuss the limitations of the research and identifies future research directions.

8.1 Achievements of the Research

Overall, the project has accomplished all the objectives initially set out in Chapter 1, with the creation of a novel transparent multimodal e-invigilation system. A series of experimental studies and evaluations have been undertaken to determine the overall effectiveness of the proposed approach. The full achievements are:

- The proposal and complete architecture design of more secure e-assessments. This novel e-invigilation system is designed in a modular fashion to incorporate a range of behavioural and physiological biometrics (the most user-friendly and robust techniques). The architecture has been designed around two operational objectives: continuous biometric-based monitoring of the participant and system-level monitoring to prevent cheating. Moreover, it offers a variety of management-level functionality that provides the basis for creating and managing assessments. This has been identified within the architectural diagram as the Data Collection Engine, Feature Extraction Engine, Biometric Profile Engine, Authentication Engine, Security Monitoring Engine, Communication Engine, and Assessment Manager respectively.

- A flexible monitoring based approach that is sat on web based service, trying to provide platform independence. The proposed client-server architecture is a platform independence design in which can be implemented via browser as it is a largely web based driven, and this makes it a lot easier in terms of usability. There would be potentially some hurdles to overcome in terms of how to build the browser compatibility with certain biometric sensors, however modern web browsers today already support functionality of capturing the camera and microphone, therefore, it is not a huge stretch to believe that future version of modification would exist that the browser can be developed in order to capture functionality of other hardware based devices also (e.g. 3D camera with infrared sensors).

- A scalable system that manages the storage, retrievals and processes of biometric samples. In terms of scalability aspect as well as a potential real time processing, the system suggests to increase and reduce the processing backend accordingly, therefore providing the elastic capacity is essential (e.g. using cloud computing platform).

- Development and implementation of a prototype with respect to the academic and student key roles, in order to highlight the ease of use and lightweight nature of the system. The focus also was on the general system requirements, architecture, database, and processes. Given the flexibility of the aforementioned architecture, a number of decisions had to be made concerning which the most transparent and robust biometric authentication to be used, what effective security restriction approaches to be applied/developed, and how to employ the most efficient software/hardware to achieve the targeted level secure e-examination and controlled monitoring. Furthermore, the prototype has focused on utilising both 2D facial recognition and the development of 3D facial authentication, and then to evaluate it in the next step. In more detail and with system snapshots, the key pages which will be used frequently by the academic have been described.

- Validation of the proposed approach. The research has experimentally explored the viability of a more secure, transparent and continuous authentication mechanism for e-assessments, which proposed in Chapter 4 and developed as a prototype in Chapter 5 of this thesis. Employing face recognitions as the most transparent multimodal (2D and 3D) biometric modalities, and novel security features through eye tracking, head movements, speech recognition, and multiple face detection to enable a robust and flexible e-invigilation approach. The results of the experiments have proven the ability of the proposed system to capture, process, and identify users through the use of biometrics. The achieved FRR has validated to a great extent the usability of the system and its ability to correctly recognise the legitimate user utilising the facial recognition in 2D and 3D modes under normal use. The capturing mechanism has been accomplished transparently during the experiments with a reliable biometric sampling process. Furthermore, the results of the implemented threat scenarios have perfectly shown the capability of the suggested approach to identify, track, and

monitor users with a view to identifying unauthorised help that could be provided by somebody else during the e-assessment.

- Evaluation of the proposed approach. A series of scenario-based evaluations to provide a comprehensive evaluation into the effectiveness of the proposed approach have also been accomplished. To evaluate all dimensions of the EIEA system, the three separate stakeholders got three separate sets of information and three separate sets of questions, in two cases it is a qualitative-based survey and the other one is a quantitative-based and qualitative-based survey. The vast majority of the interview/feedback outcomes of the three stakeholders can be considered as positive, constructive and valuable.

8.2 Limitations of the Research Project

The objectives of the research project have been met, however, as with any system under development; there are some limitations are identified including:

1- The limited number of expert participants. During the participant recruitment in the evaluation stage, the researcher invited 81 experts, 16 of them responded and accepted the invitation after sending the first email, however only 5 of them were interviewed, this due to that 11 of the responded experts have never specified the date and time for conducting the interview. 16 experts apologised, but 49 did not respond to the invitation at all.

2- The researcher decided to implement the experiment involving many participants individually rather than groups, this decision has been made due to the hardware and software requirements which were very difficult to be achieved within the managed Plymouth University limitations, as the installed devices need verity of special hardware and software specifications. Furthermore, at the time of conducting the experiment, it was not possible to buy many computers with a built-in 3D camera, as it was not available yet, which might make conducting the experiment far easier.

3- Only 12 of the 15 predefined threat scenarios has been involved, this due to the difficulty of implementing the 13th scenario while the designed prototype was not able to implement the 14th and 15th scenarios. However, the theoretical design of the architecture would normally control all the 15 threat scenarios.

8.3 Suggestions and Scope for Future Work

This research programme has advanced the field of identity verification and security for e-assessments. Nevertheless, there are several areas in which future work could be carried out to advance upon what has been achieved in this research. These include:

1- There was a limitation in the availability of biometric modalities, future work needs to focus upon, when available, introducing additional biometric modalities and understanding the relationship that can have and supporting and improving upon the recognition performance of the underlined system.
2- Test the proposed models in a real environment. This aims to measure their security and applicability, as well as acceptance.
3- Deploy a complete version of the suggested EIEA system on the cloud to provide them with the required computational power and evaluate the improvement in performance. This includes storage, memory and CPU usage that might be rented in lower costs.
4- There is an excellent opportunity to utilise the collected data of both eye tracking and head movement in order to explore the possibility of producing a novel and new biometric modalities.
5- The captured left and right eye images could be utilised to explore the possibility to achieve sclera or iris recognition modalities. Furthermore, these photos (if the number of the collected photos was large enough) can even be used to accomplish eye movement analysis for both security and authenticity purposes.
6- Examine the possibility of utilising the captured sentences (the text sentences that collected during the speech recognition JSFG) for accomplishing transplant linguistic analysis.

References

1. Abaza, A., A., R., Hebert, C., Harrison, M. and Nixon, M. (2013) ‘A survey on ear biomet-rics.’, *ACM Computing Surveys*, 45(2), pp. 1–35.
2. Agency, U. B. (2014) *Changes to English language certification for visa applications - News articles - GOV.UK*. Available at: https://www.gov.uk/government/world-location-news/changes-to-english-language-certification-for-visa-applications--3 (Accessed: 21 October 2014).
3. Ahmed, A. A. E. and Traore, I. (2007) ‘A New Biometric Technology Based on Mouse Dynamics’, *IEEE Transactions on Dependable and Secure Computing*, 4(3), pp. 165–179. doi: 10.1109/TDSC.2007.70207.
4. Ahmed, A. and Traore, I. (2014) ‘Biometric Recognition Based on Free-Text Keystroke Dynamics’, *IEEE transactions on cybernetics*, 44(4), pp. 1–15.
5. Al-harby, F., Qahwaji, R. and Kamala, M. (2004) *Secure Biometrics Authentication : A brief review of the Literature*. Bradford.
6. Al-Hudhud, G., Abdulaziz Alzamel, M., Alattas, E. and Alwabil, A. (2014) ‘Using brain signals patterns for biometric identity verification systems’, *Computers in Human Behavior*. Elsevier Ltd, 31, pp. 224–229. doi: 10.1016/j.chb.2013.09.018.
7. Al-Smadi, M., Hoefler, M. and Guetl, C. (2011) ‘An Integrated Model for E-Assessment of Learning Experiences Enriched with Complex Learning Resources’, in *Proceedings 3rd IEEE International Conference on Intelligent Networking and Collaborative Systems INCoS*. Fukuoka: Ieee, pp. 824–829. doi: 10.1109/INCoS.2011.52.
8. AL-Smadi, M., Hofler, M. and Guetl, C. (2011) ‘Integrated and enhanced e-assessment forms for learning: Scenarios from alice project’, in *14th International Conference on Interactive Collaborative Learning (ICL), 2011*. Piestany: IEEE, pp. 626–631.
9. Alasuutari, P. (2009) ‘The rise and relevance of qualitative research’, *International Journal of Social Research Methodology*, 13, pp. 139–155. Available at: http://dx.doi.org/10.1080/13645570902966056.
10. Albin, T., Plains, H. and Services, E. (2008) ‘Comfortable Portable Computing: The Ergonomic Equation’, pp. 1–19. Available at: www.ergotron.com.
11. Alotaibi, S. (2010) ‘Using biometrics authentication via fingerprint recognition in e-exams in e-learning environment’, in *The 4th Saudi International Conference*.
12. Alotaibi, S. J. and Argles, D. (2011) ‘FingerID: A new security model based on fingerprint recognition for personal learning environments (PLEs)’, in *2011 IEEE Global Engineering Education Conference (EDUCON)*. Amman: Ieee, pp. 142–151. doi: 10.1109/EDUCON.2011.5773128.
13. Alwi, N. H. M. and Fan, I. S. (2010) ‘Information Security Threats Analysis for e-Learning’, in *Proceedings of the First International Conference TECH- EDUCATION*. Athens, Greece, pp. 285–291.
14. Amazon (2017) *Amazon Web Services Simple Monthly Calculator*. Available at: https://calculator.s3.amazonaws.com/index.html (Accessed: 23 April 2017).
15. Anil K. Jain, Patrick Flynn, A. A. R. (2008) *Handbook of Biometrics*. Springer

Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA.

16. Apampa, K. (2010) *Presence verification for summative e-assessments*. UNIVERSITY OF SOUTHAMPTON.
17. Apampa, K., Wills, G. and Argles, D. (2009) 'Towards security goals in summative e-assessment security', in IEEE (ed.) *Institute of Electrical and Electronics Engineers*. London, pp. 1–5.
18. Apampa, K., Wills, G. and Argles, D. (2010a) 'An approach to presence verification in summative e-assessment security', in *Information Society (i-Society)*. London: IEEE, pp. 647–651.
19. Apampa, K., Wills, G. and Argles, D. (2010b) 'User security issues in summative e-assessment security', *International Journal of Digital Society (IJDS)*, 1(2), pp. 135–147.
20. Apampa, K., Wills, G. and Argles, D. (2011) 'Towards a blob-based presence verification system in summative e-assessments', *International Journal of e-Assessment*, 1(1), pp. 1–17.
21. Apampa, K., Zhang, T., Wills, G. and Argles, D. (2008) 'Ensuring privacy of biometric factors in multi-factor authentication systems', in *International Conference on Security and Cryptography in ICETE 08*. Porto.
22. Arbab-Zavar, B. and Nixon, M. (2011) 'On guided model-based analysis for ear biometrics', *Computer Vision and Image Understanding*, 115(4), pp. 487–502.
23. Asha, S. and Chellappan, C. (2008) 'Authentication of e-learners using multimodal biometric technology', in *2008 International Symposium on Biometrics and Security Technologies*. Islamabad: Ieee, pp. 1–6. doi: 10.1109/ISBAST.2008.4547640.
24. Aupy, A. and Clarke, N. (2005) 'User Authentication by Service Utilisation Profiling', in *Proceed-ngs of the ISOneWorld 2005*. Las Vegas, USA.
25. AxxonSoft (2011) *Face Recognition*. Available at: http://www.axxonsoft.com/integrated%0A_security_solutions/face_recognition/index.php?phrase_id=3032106 (Accessed: 9 August 2014).
26. Babich, A. (2012) *Biometric Authentication . Types of biometric identifiers*. University of Applied Science.
27. Baghdad University (2014) *English language certification*. Available at: http://www.cc.uobaghdad.edu.iq/ (Accessed: 21 October 2014).
28. Bailie, J. and Jortberg, M. (2009) 'Online learner authentication: Verifying the identity of online users', *Journal of Online Learning and Teaching*, 5(2), p. 25.
29. Bal, A. and Acharya, A. (2011) 'Biometric authentication and tracking system for online examination system', in *International Conference on Recent Trends in Information Systems*. Kolkata: Ieee, pp. 209–213. doi: 10.1109/ReTIS.2011.6146869.
30. Besbes, F., Trichili, H. and Solaiman, B. (2008) 'Multimodal biometric system based on fingerprint identification and iris recognition', in IEEE (ed.) *I3rd International Conference on nformation and Communication Technologies: From Theory to Applications, ICTTA*. Damascus, pp. 1–5.
31. Biella, D., Engert, S. and Huth, D. (2009) *Design and delivery of an E-assessment solution at the University of Duisburg-Essen, Centre for Information and Media Services, University of Duisburg-Essen, Schuetzenbahn 70, 45127 Essen, Germany*.

Essen.

32. Biometric Security (2014) *BiometricSecurity - Development*. Available at: http://biometricsecurity.wikispaces.com/Development (Accessed: 1 October 2014).
33. Biometrics Institute (2013) *Biometrics Institute Industry Survey 2013, 1-6*.
34. Blinco, K., Mason, J., McLean, N. and Wilson, S. (2004) *Trends and issues in e-learning infrastructure development*, *Altilab04, Redwood City, California, USA*.
35. Bonissi, A., Labati, R., Perico, L. and Sassi, R. (2013) 'A preliminary study on continuous authentication methods for photoplethysmographic biometrics', in *IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS),*. doi: 10.1109/BIOMS.2013.6656145.
36. Bours, P. and Barghouthi, H. (2009) 'Continuous Authentication using Biometric Keystroke Dynamics Patrick Bours and Hafez Barghouthi', in *The Norwegian Information Security Conference (NISK) 2009*. Teknologivegen, pp. 1–12.
37. Bours, P. and Fullu, C. J. (2009) 'A Login System Using Mouse Dynamics', in *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Kyoto: Ieee, pp. 1072–1077. doi: 10.1109/IIH-MSP.2009.77.
38. Bushweller, K. (1999) 'Generation of cheaters', *The American School Board Journal*, 186(4), pp. 24–32.
39. Carlisle, M. and Baird, L. (2007) 'Design and Use of a Secure testing Environment on Untrusted Hardware', in *Information Assurance and Security Workshop*. West Point, NY: IEEE, pp. 349–354.
40. Ceccarelli, A., Montecchi, L., Brancati, F., Lollini, P., Marguglio, A. and Bondavalli, A. (2014) 'Continuous and Transparent User Identity Verification for Secure Internet Services', *IEEE Transactions on Dependable and Secure Computing,* pp(99), pp. 1–14. doi: 10.1109/TDSC.2013.2297709.
41. Chang, K. I., Bowyer, K. W., Flynn, P. J. and Dame, N. (2010) 'Multi-Modal 2D and 3D Biometrics for Face Recognition', in *IEEE International Workshop on Analysis and Modeling of Faces and Gestures, 2003. AMFG 2003.* Nice, France, pp. 187–194.
42. Chang, W., Kim, K. E. and Lee, H. (2006) 'Recognition of Grip-Patterns by Using Capacitive Touch Sensors', in *IIEEE International Symposium on ndustrial Electronics, 2006*. Montreal, Que., pp. 2936–2941.
43. Chaos Computer Club (2014) *Fingerprint Biometrics hacked again*, *Chaos Communication Congress (31C3)*. Available at: http://www.ccc.de/en/updates/2014/ursel (Accessed: 10 March 2015).
44. Chen, W.-K., Lee, J.-C., Han, W.-Y., Shih, C.-K. and Chang, K.-C. (2012) 'Iris recognition based on bidimensional empirical mode decomposition and fractal dimension', *Information Sciences*. Elsevier Inc., 221, pp. 439–451. doi: 10.1016/j.ins.2012.09.021.
45. Chew, W. J., Seng, K. P., Liau, H. F. and Ang, L. (2009) 'New 3D Face Matching Technique for 3D Model Based Face Recognition', in *International Symposium on Intelligent Signal Processing and Communications Systems, 2008. ISPACS 2008*, pp. 2008–2011.
46. Chikkerur, S., Pankanti, S., Jea, A., Ratha, N. and Bolle, R. (2006) 'Fingerprint representation using localized texture features', in *The 18th International Conference on*

Pattern Recognition (ICPR'06). IEEE, p. 4. doi: 10.1109/ICPR.2006.576.

47. Clarke, N. (2011) *Transparent user authentication: biometrics, RFID and behavioural profiling*. London: Springer London. doi: 10.1007/978-0-85729-805-8.
48. Clarke, N. and Furnell, S. (2005) 'Biometrics–The promise versus the practice', *Computer Fraud & Security*, pp. 12–16.
49. Clarke, N. and Furnell, S. (2006) 'A composite user authentication architecture for mobile devices', *Journal of Information Warfare*, 5(2), pp. 11–29.
50. Clarke, N., Karatzouni, S. and Furnell, S. (2008) 'Transparent facial recognition for mobile devices', in *Proceedings of the 7th Security Conference*. Las Vegas, USA.
51. Clarke, N., Karatzouni, S. and Furnell, S. (2009) 'Flexible and Transparent User Authentication for Mobile Devices', in *Gritzalis D And Lopez J (ed) Emerging Challenges for Security, Privacy and Trust, 24th IFIP TC 11 International Information Security Conference*. Pafos, Cyprus, pp. 1–12.
52. Clarke, N. L., Dowland, P. and Furnell, S. M. (2013) 'e-Invigilator: A Biometric-Based Supervision System for e-Assessments', in *IInternational Conference on nformation Society (i-Society), 2013*. Toronto, p. 5.
53. Clarke, N. L. and Furnell, S. M. (2007) 'Advanced user authentication for mobile devices', *Computers & Security*, 26(2), pp. 109–119. doi: 10.1016/j.cose.2006.08.008.
54. Clarke, N. L. and Mekala, A. R. (2007) 'The application of signature recognition to transparent handwriting verification for mobile devices', *Information Management & Computer Security*, 15(3), pp. 214–225. doi: 10.1108/09685220710759559.
55. Classifiers, A. and Engineering, M. (2009) 'Keystroke Pressure Based Typing Biometrics Authentication System by Combining ANN and', in *International Conference on Computer and Communication Engineering (ICCCE), 2010*. Kuala Lumpur, pp. 198–203.
56. Commission Nationale (2001) *A Century of Biometrics, 1-13*.
57. Commons, W. (2014) *File:PSM V63 D402 Left palm print uninterpreted.png - Wikimedia Commons*. Available at: http://commons.wikimedia.org/wiki/File:PSM_V63_D402_Left_palm_print_uninterpreted.png (Accessed: 2 October 2014).
58. Coursera (2014) *Coursera*. Available at: https://www.coursera.org/ (Accessed: 29 September 2014).
59. Crawford, H. (2012) *A framework for continuous, transparent authentication on mobile devices*. University of Glasgow.
60. Crawford, H. and Renaud, K. (2014) 'Understanding User Perceptions of Transparent Authentication on a Mobile Device', *Journal of Trust Management*, 1(7), pp. 1–28. doi: 10.1186/2196-064X-1-7.
61. Crawford, H., Renaud, K. and Storer, T. (2013) 'A framework for continuous, transparent mobile device authentication', *Computers & Security*. Elsevier Ltd, 39, pp. 127–136. doi: 10.1016/j.cose.2013.05.005.
62. Creswell, J. W. (2007) 'Qualitative inquiry & research design: Choosing among five approaches', in. Sage, Thousand Oaks, CA.
63. Creswell, J. W. (2013) *Research Design: Qualitative, Quantitative, and Mixed Methods*

Approaches. Thousand Oaks: SAGE Publications.

64. Crisp, G. (2011) *Teacher ' s Handbook on e-Assessment*. Sydney: the Creative Commons Attribution-Noncommercial- ShareAlike 3.0 Australia Licence.
65. Cummings, A., MS, N. and JN, C. (2010) 'A Novel Ray Analogy for Enrolment of Ear Biometrics', in *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE Interna-tional Conference on Biometrics Compendium, IEEE*. Washington, DC.
66. D, U. and Williams, G. (1985) 'Identity verification through keyboard characteristics', *International Journal of Man-Machine Studies*, 23(3), pp. 263–273.
67. Das, A. K. (2011) 'Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards', *IET Information Security*, 5(3), p. 145. doi: 10.1049/iet-ifs.2010.0125.
68. Daugman, J. (2003) 'The importance of being random: statistical principles of iris recognition', *Pattern Recognition*, 36(2), pp. 279–291. doi: 10.1016/S0031-3203(02)00030-4.
69. Daugman, J. (2007) 'New methods in iris recognition', *IEEE transactions on systems and cybernetics - Part B, Cybernetics*, 37(5), pp. 1167–75.
70. Daugman, J. G. (1993) 'High confidence visual recognition of persons by a test of statistical independence', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11), pp. 1148–1161. doi: 10.1109/34.244676.
71. Dell (2017) *Dell Online Server Prices*. Available at: http://www.dell.com/uk/business/p/enterprise-deals#poweredge-tower-server-deals?lnktrgt=parent (Accessed: 23 April 2017).
72. Denning, D. (1999) *Information Warfare & Security*. ACM Press.
73. Dick, M., Sheard, J., Bareiss, C., Carter, J., Joyce, D., Harding, T. and Laxer, C. (2003) 'Addressing Student Cheating: Definitions and Solutions', *ACM Special Interest Group on Computer Science Education Bulletin*, 35(2), pp. 172–184.
74. Du, Y. (2006) 'Review of iris recognition: cameras, systems, and their applications', *Sensor Review*, 26(1), pp. 66 – 69.
75. EISENBERG, A. (2013) *Keeping an Eye on Online Test-Takers*. Available at: http://www.nytimes.com/2013/03/03/technology/new-technologies-aim-to-foil-online-course-cheating.html?adxnnl=1&adxnnlx=1413932530-4YAAwNVDAgl5JNAakYDH1A (Accessed: 21 October 2014).
76. EPIC (2005) *Biometric Comparison Guide*. Available at: http://epic.org/privacy/%0Asurveillance/spotlight/1005/irid_guide.pdf, (Accessed: 22 September 2014).
77. Eveno, N. and Besacier, L. (2005) 'Co-inertia analysis for "liveness" test in audio-visual biometrics', in *ISPA 2005. Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis, 2005.* Ieee, pp. 257–261. doi: 10.1109/ISPA.2005.195419.
78. Everitt, R. and McOwan, P. (2003) 'Java-Based Internet Biometric Authentication System', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(9), p. 1166–1172.
79. Face-rec (2011) *Vendors*. Available at: http://www.face-rec.org/vendors/ (Accessed: 7

May 2015).

80. Fadhel, N., Wills, G. and Argles, D. (2011) 'Transparent authentication in E-learning', in *International Conference on Information Society (i-Society)*. London: IEEE, pp. 336–342.
81. Fahmi, A., Kodirov, E., Choi, D. and Lee, G. (2012) 'Implicit Authentication based on Ear Shape Biometrics using Smartphone Camera during A Call', in *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. Seoul, Korea, pp. 2272–2276.
82. Farnese, M. L., Tramontano, C., Fida, R. and Paciello, M. (2011) 'Cheating Behaviors in Academic Context: Does Academic Moral Disengagement Matter?', *Procedia - Social and Behavioral Sciences*, 29(2010), pp. 356–365. doi: 10.1016/j.sbspro.2011.11.250.
83. Feher, C., Elovici, Y., Moskovitch, R., Rokach, L. and Schclar, A. (2012) 'User identity verification via mouse dynamics', *Information Sciences*. Elsevier Inc., 201, pp. 19–36. doi: 10.1016/j.ins.2012.02.066.
84. Ferreira, J. and Santos, H. (2012) 'Keystroke dynamics for continuous access control enforcement', in *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012*. Sanya: IEEE. doi: 10.1109/CyberC.2012.43.
85. Flior, E. and Kowalski, K. (2010) 'Continuous Biometric User Authentication in Online Examinations', in *2010 Seventh International Conference on Information Technology: New Generations*. Las Vegas: Ieee, pp. 488–492. doi: 10.1109/ITNG.2010.250.
86. Flom, L. and Safir, A. (1987) 'Iris Recognition System'. USA. Available at: file:///C:/Users/ssketab/Desktop/US4641349.pdf.
87. Franklin, M. I. (2013) *Understanding Research: Coping with the Quantitative-Qualitative Divide*. London and New York: Routledge.
88. Free-press-release (2011) *Facial Recognition Emerging as the Fastest Growing Segment*. Available at: http://www.free-press-release.com/news-facial-recognition-emerging-as-the-fastest-growing-segment-1295508190.html (Accessed: 23 February 2015).
89. Gaines R, Lisowski W, Press S, S. N. (1980) 'Authentication by keystroke timing: some preliminary results', *RAND CORP SANTA MONICA CA (No. RAND-R-2526-NSF)*, pp. 1–51.
90. Galbally, J., Ortiz-lopez, J., Fierrez, J. and Ortega-garcia, J. (2012) 'Iris Liveness Detection Based on Quality Related Features', in *5th IAPR International Conference on Biometrics Compendi-um, IEEE Biometrics (ICB). IEEE*, pp. 271 – 276.
91. Gamboa, H. and Fred, A. (2003) 'An identity authentication system based on human computer interaction behavior', in *Pattern Recognition in Information Systems, Proceedings of the 3rd International Workshop on Pattern Recognition in Information Systems*. PRIS, France.
92. Gamboa, H. and Fred, A. (2004) 'A behavioural biometric system based on human computer interaction', in *In SPIE 5404 - Biometric Technology for Human Identification*. Orlando, FL USA, pp. 381–392.
93. Gao, Q. (2012) 'Biometric Authentication to Prevent e-Cheating', *International Journal of Instructional Technology and Distance Learning*, 9(2), p. 93.
94. Geekosystem (2011) *Facebook Will Go Ahead and Scan Your Face Now*. Available at: https://www.themarysue.com/facebook-face-recognition/ (Accessed: 18 March 2015).

95. Gilbert, L., Gale, V., Warburton, B. and Wills, G. (2009) *Report on Summative E-Assessment Quality (REAQ)*.

96. Giorgi, A. (2009) *The Descriptive Phenomenological Method in Psychology*. Duquesne University Press: Pittsburgh, PA.

97. Given, L. M. (2008) *The Sage encyclopedia of qualitative research methods*. Los Angeles: Calif.: Sage Publications.

98. Gosset P (1998) *ASPeCT: Fraud Detection Concepts: Final Report*. Available at: http://www.chrismitchell.net/ASPeCT/CD Data/Deliverables/D18.pdf.

99. Guse, D. (2011) *Gesture-based User Authentication on Mobile Devices using Accelerometer and Gyroscope. Berlin Institute of Technology*.

100. Hayes, B. and Ringwood, J. (2008) 'Student Authentication for Oral Assessment in Distance Learning Programs', *IEEE Transactions on Learning Technologies,* 1(3), pp. 165–175.

101. Hayes, B. and Ringwood, J. (2009) 'Authenticating student work in an e-learning programme via speaker recognition', in *2009 3rd International Conference on Signals, Circuits and Systems (SCS)*. Medenine: Ieee, pp. 1–6. doi: 10.1109/ICSCS.2009.5412484.

102. Hentea, M., Shea, M. J. and Pennington, L. (2003) 'A Perspective on Fulfilling the Expectations of Distance Education', in *Proceedings of the 4th Conference on Information Technology Curriculum (CITC4) Lafayette*. Lafayette, Indiana, USA, pp. 160–167.

103. Hernández, J. a., Ortiz, a. O., Andaverde, J. and Burlak, G. (2008) 'Biometrics in Online Assessments: A Study Case in High School Students', in *18th International Conference on Electronics, Communications and Computers (conielecomp 2008)*. Puebla: Ieee, pp. 111–116. doi: 10.1109/CONIELECOMP.2008.36.

104. HESA UK (2017) *Higher Education Statistics Agency*. Available at: https://m.hesa.ac.uk/uk-he-stats/?p=institution&y=15/16&l=P&g=&s=&n=1 (Accessed: 16 April 2017).

105. Holland, C. D., Komogortsev, O. V and Tx, S. M. (2012) 'Biometric Verification via Complex Eye Movements : The Effects of Environment and Stimulus', pp. 39–46.

106. Holland, C. and Komogortsev, O. V (2011) 'Biometric Identification via Eye Movement Scan paths in Reading', pp. 1–8.

107. Howell, K. E. (2013) 'Introduction to the Philosophy of Methodology', *London: Sage Publications*.

108. Hurley, D., Nixon, M. and Carter, J. (2005) 'Force field feature extraction for ear biometrics', *Comput. Vis. Image Understand.*, 98, pp. 491–512.

109. Hwang, S., Cho, S. and Park, S. (2009) 'Keystroke dynamics-based authentication for mobile devices', *Computers & Security*. Elsevier Ltd, 28(1–2), pp. 85–93. doi: 10.1016/j.cose.2008.10.002.

110. Indeamart (2014) *Fingerprint Security Systems - eNBioScan - C1 Manufacturer & Exporter from Pune*. Available at: http://www.indiamart.com/bioenabletech/fingerprint-security-systems.html (Accessed: 21 October 2014).

111. Intel (2016) *Intel RealSense*. Available at:

http://www.intel.co.uk/content/www/uk/en/architecture-and-technology/realsense-overview.html (Accessed: 4 October 2016).

112. Irfan, C. M. A., Nomura, S., Ouzzane, K. and Fukumura, Y. (2009) 'Face-Based Access Control and Invigilation Tool for E-learning Systems', in *2009 International Conference on Biometrics and Kansei Engineering*. Cieszyn: Ieee, pp. 40–44. doi: 10.1109/ICBAKE.2009.43.

113. Ishak, I. S. and Alias, R. A. (2005) 'Designing a Strategic Information Systems Planning Methodology for Malaysian Institutes of Higher Learning', *Issues in Information Systems*, VI(1).

114. ISO (2006a) *ISO/IEC 19784-1:2006 - Information technology -- Biometric application programming interface -- Part 1: BioAPI specification*. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33922 (Accessed: 21 January 2015).

115. ISO (2006b) *ISO/IEC 19785-1:2006 - Information technology -- Common Biometric Exchange Formats Framework -- Part 1: Data element specification*. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41047 (Accessed: 21 January 2015).

116. ISO (2011) *ISO/IEC 19794-1:2011 - Information technology -- Biometric data interchange formats -- Part 1: Framework*. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50862 (Accessed: 21 January 2015).

117. ISO: ISO/IEC 19785-1:2006 (2006) *Information technology – common biometric exchange formats framework – part 1: data element specification*.

118. ISO: ISO/IEC 19794-5 (2009) *Information technology – biometric data interchange formats – part 5: face image data*.

119. IT Parks Update (2014) *ICFOSS, IIITM-K 3-day Programme for Academic & Research Institutions | IT Parks Update*. Available at: http://itparksupdate.in/icfoss-iiitm-k-3-day-programme-for-academic-research-institutions/ (Accessed: 25 November 2014).

120. Jain, A., Hong, L. and Pankanti, S. (2000) 'Biometric identification', *Communications of the ACM*, 43(2).

121. Jain, A., Hong, L., Pankanti, S. and Bolle, R. (1997) 'An identity-authentication system using fingerprints', *Proceedings of the IEEE*, 85(9).

122. Jiawei, H., Liangrui, P. and Li, Z. (2015) 'XFace: A Face Recognition System for Android Mobile Phones', in *3rd International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), 2015 IEEE*.

123. Jorgensen, Z. and Yu, T. (2011) 'On mouse dynamics as a behavioral biometric for authentication', *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS '11*. New York, New York, USA: ACM Press, p. 476. doi: 10.1145/1966913.1966983.

124. Joyce, R. and Gupta, G. (1990) 'Identity authentication based on keystroke latencies', *Communications of the ACM*, 33(2), pp. 168–176. doi: 10.1145/75577.75582.

125. JSGFGrammar (2016) *Class JSGFGrammar*. Available at: http://cmusphinx.sourceforge.net/doc/sphinx4/edu/cmu/sphinx/jsgf/JSGFGrammar.html (Accessed: 5 October 2016).

126. JTC1/SC (2013) *BUSINESS PLAN FOR JTC 1/SC 37 'BIOMETRICS' for the PERIOD COVERED: October 2012 - September 2013*.

127. Jung, I. and Yeom, H. (2009) 'Enhanced security for online exams using group cryptography', *IEEE Transactions on Education,* 52(3), pp. 340–349.

128. Jung, J., Bien, Z., Lee, S. and Sato, T. (2003) 'Dynamic-footprint based person identification using mat-type pressure sensor', in *Proceedings of the 2Sa Annual lntemational Conference of the IEEE EMBS Cancun*. Mexico, pp. 2937–2940.

129. Karnan, M., Akila, M. and Krishnaraj, N. (2011) 'Biometric personal authentication using keystroke dynamics: A review', *Applied Soft Computing*. Elsevier B.V., 11(2), pp. 1565–1573. doi: 10.1016/j.asoc.2010.08.003.

130. Kasprowski, P. and Ober, J. (2004) 'Eye movements in biometrics', *In Biometric Authentication Springer-Verlag*, 3087, p. 248–258.

131. Kasprowski, P. and Ober, J. (2004) 'Eye Movements in Biometrics 2 Physiology of Eye Movements 3 Previous Researches Concerning Eye Movements', pp. 248–258.

132. Ketab, S. S., Clarke, N. L. and Dowland, P. S. (2015) 'E-Invigilation Of E-Assessments', in *Proceedings of INTED2015 Conference*. Madrid, pp. 1582–1591.

133. Khan, M. and Tsai, P. (2011) 'Biometric driven initiative system for passive continuous authentication', in *7th International Conference on Information Assurance and Security (IAS), 2011*. Melaka: IEEE, pp. 139–144.

134. Kikuchi, S., Furuta, T. and Akakura, T. (2008) 'Periodical examinees identification in e-test systems using the localized arc pattern method', in *Distance Learning and the Internet Conference 2008*, p. 8.

135. Ko, C. C. and Cheng, C. D. (2004) 'Secure Internet examination system based on video monitoring', *Internet Research*, 14(1), pp. 48–61. doi: 10.1108/10662240410516318.

136. Ko, C. C. and Cheng, C. D. (2008) 'Flexible and Secure Computer-Based Assessment Using a Single Zip Disk', *Computers & Education*, 50(3), pp. 915–926. doi: 10.1016/j.compedu.2006.09.010.

137. Kong, A., Zhang, D. and Kamel, M. (2006) 'Palmprint identification using feature-level fusion', *Pattern Recognition*, 39(3), pp. 478–487. doi: 10.1016/j.patcog.2005.08.014.

138. Kryterion (2014a) *Kryterion*. Available at: http://kryteriononline.com/ (Accessed: 29 September 2014).

139. Kryterion (2014b) *Security | Kryterion*. Available at: http://kryteriononline.com/testing-platform/security/ (Accessed: 29 September 2014).

140. Kryterion (2014c) *Testing Platform | Kryterion*. Available at: http://kryteriononline.com/testing-platform/ (Accessed: 29 September 2014).

141. Kumar, A., Garg, S. and Hanmandlu, M. (2014) 'Biometric authentication using finger nail plates', *Expert Systems with Applications*. Elsevier Ltd, 41(2), pp. 373–386. doi: 10.1016/j.eswa.2013.07.057.

142. Kumar, A., Wong, D. C. M., Shen, H. C. and Jain, A. K. (2006) 'Personal authentication using hand images', *Pattern Recognition Letters*, 27(13), pp. 1478–1486. doi: 10.1016/j.patrec.2006.02.021.

143. Kumar, A., Wong, D., Shen, H. and Jain, A. (2003) 'Personal verification using palmprint and hand geometry biometric', in *Audio-and Video-Based ...*, pp. 668–678.

doi: 10.1007/3-540-44887-X_78.

144. Kumar, A. and Zhang, D. (2005) 'Personal authentication using multiple palmprint representation', *Pattern Recognition*, 38(10), pp. 1695–1704. doi: 10.1016/j.patcog.2005.03.012.

145. Kuzel, A. J. (1999) 'Sampling in Qualitative Inquiry', in *BF Crabtrree and WL Miller (Eds.) Doing Qualitative Research (2nd ed.)*. Sage, Thousand Oaks, CA, pp. 33–45.

146. Lai, K., Konrad, J. and Ishwar, P. (2012) 'Towards gesture-based user authentication', in *2012 IEEE Ninth International Conference onAdvanced Video and Signal-Based Surveillance (AVSS),*. Beijing: IEEE, pp. 282–287. doi: 10.1109/AVSS.2012.77.

147. Levy, Y. and Ramim, M. (2007) *A theoretical approach for biometrics authentication of e-exams*, *Research, The Open University of Israel, ...*. Nova.

148. Levy, Y. and Ramim, M. (2009) 'Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM)', *Interdisciplinary Journal of E-learning and Learning Objects*, 5, p. 19.

149. Levy, Y., Ramim, M. M., Furnell, S. M. and Clarke, N. L. (2010) 'Comparing Intentions to Use Multibiometric Authentication in Online Exams E-learning', *E-learning Systems Security*, 28(2), pp. 102–113. doi: http://dx.doi.org/10.1108/10650741111117806.

150. Li, F. (2012) *Behaviour Profiling for Mobile Devices*. University of Plymouth.

151. Li, F., Clarke, N., Papadaki, M. and Dowland, P. (2011) 'Behaviour Profiling for Transparent Authentication for Mobile Devices', in *the 10th European Conference on Information Warfare and Security (ECIW 2011)*. Tallinn, Estonia, pp. 307–314.

152. Li, F., Clarke, N., Papadaki, M. and Dowland, P. (2013) 'Active authentication for mobile devices utilising behaviour profiling', *International Journal of Information Security*, 13(3), pp. 229–244.

153. Lin, N. H., Korba, L., Yee, G., Shih, T. K. and Lin, H. W. (2004) 'Security and privacy technologies for distance education applications', *18th International Conference on Advanced Information Networking and Applications, 2004. AINA 2004.* Ieee, 1, pp. 580–585. doi: 10.1109/AINA.2004.1283972.

154. Liu, J., Sun, Z. and Tan, T. (2013) 'Recognition of motion blurred iris images', *IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2013*. doi: 10.1109/BTAS.2013.6712691.

155. Lívia C. F. Araújo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga, Lee L. Ling, andJoão B. T. Y.-U. (2005) 'User Authentication Through Typing Biometrics Features', *IEEE TRANSACTIONS ON SIGNAL PROCESSING*, 53(2), pp. 851–855.

156. Loyola-González, O., Pérez, M. A. M., Rodriguez, A. E. G. and Borroto, M. G. (2015) *A Framework in C# for Fingerprint Verification*. Available at: http://www.codeproject.com/Articles/97590/A-Framework-in-C-for-Fingerprint-Verification (Accessed: 12 July 2015).

157. Lu, Y.-C., Yang, Y.-S., Chang, P.-C. and Yang, C.-S. (2013) 'The design and implementation of intelligent assessment management system', in *2013 IEEE Global Engineering Education Conference (EDUCON)*. Berlin: Ieee, pp. 451–457. doi: 10.1109/EduCon.2013.6530144.

158. Luminita, D. C. (2011) 'Information security in E-learning Platforms', *Procedia - Social and Behavioral Sciences*. Elsevier B.V., 15, pp. 2689–2693. doi:

10.1016/j.sbspro.2011.04.171.

159. Mahmud, K. and Gope, K. (2009) 'Challenges of Implementing E-learning for Higher Education in Least Developed Countries: A Case Study on Bangladesh', in *2009 International Conference on Information and Multimedia Technology*. Jeju Island: Ieee, pp. 155–159. doi: 10.1109/ICIMT.2009.27.

160. Maltoni, D., Maio, D., Jain, A. and Prabhakar, S. (2009) *Handbook of fingerprint recognition*. London, UK: Springer.

161. Marais, E. (2006) 'Security issues specific to E-assessments', in *8th Annual Conference on WWW Applications*.

162. Marcus, A., Raul, J., Ramirez-Velarde, R. and Nolazco-Flores, J. (2008) 'Addressing Secure Assessments for Internet-Based Distance Learning Still an Irresolvable Issue', in *Proceedings of the 9th Latin-American Congress of Educational Computing*. Caracas, Venezuela.

163. MarketsandMarkets (2011) *Global Biometrics Technology Market (2010-2015) – Market Forecast by Products, End-User Application and Geography*.

164. MarketsandMarkets (2014) 'Next Generation Biometric Market – By Technology, Function, Application, & Geography (2014-2020)'.

165. Matta, F. and Dugelay, J.-L. (2009) 'Person recognition using facial video information: A state of the art', *Journal of Visual Languages & Computing*. Elsevier, 20(3), pp. 180–187. doi: 10.1016/j.jvlc.2009.01.002.

166. McCabe, D. (2005) 'Cheating among college and university students: A North American perspective', *International Journal for Educational Integrity*, 1(1).

167. Meshoul, S. and Batouche, M. (2010) 'Combining Fisher Discriminant Analysis and probabilistic neural network for effective on-line signature recognition', in *10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA)*. Kuala Lumpur: IEEE, pp. 658–661.

168. Michael, G. K. O., Connie, T. and Teoh, A. B. J. (2012) 'A contactless biometric system using multiple hand features', *Journal of Visual Communication and Image Representation*. Elsevier Inc., 23(7), pp. 1068–1084. doi: 10.1016/j.jvcir.2012.07.004.

169. Mir, A., Rubab, S. and Jhat, Z. (2011) 'Biometrics verification: a literature survey', *International Journal of Computing and ICT Research*, 5(2), pp. 67–80.

170. Moini, A. and Madni, A. (2009) 'Leveraging biometrics for user authentication in online learning: a systems perspective', *IEEE Systems Journal*, 3(4), pp. 469–476.

171. Monitgomery, T. M. (2014) *Anatomy, Physiology and Pathology of the Human Eye*. Available at: http://www.tedmontgomery.com/the_eye/indexiris.html (Accessed: 12 March 2014).

172. Montalv, J., Garcia, R. and Bezerra, M. A. (2014) 'Empirical keystroke analysis in passwords', in *5th ISSNIP-IEEE Biosignals and Biorobotics Conference (2014): Biosignals and Robotics for Better and Safer Living (BRC)*. IEEE.

173. Moreno, B. and Sanchez, A. (1999) 'On the use of outer ear images for personal identification in security applications', in *Proceedings of IEEE 33rd Annual International Conference on Security Technologies*. Madrid, pp. 469–476.

174. Morse, J. M. (2000) 'Determining sample size', *Qualitative Health Research*, 10(1), pp.

3–5.

175. Mothukuri, U. (2012) ‘Invigilated online assessment: Various ways to minimize unauthorized help’, in *IEEE Symposium on E-Learning, E-Management and E-Services (IS3e),*. Kuala Lumpur: IEEE, pp. 1–4.

176. N.M.Gunathilake, A.P.B.Padikaraarachchi, S.P.Koralagoda, M. Gj., P.A.I.M.Paliyawadana, Manawadu, C. D. and Rajapaksha, U. U. S. (2013) ‘Enhancing the security of online banking systems via keystroke dynamics’, in *The 8th International Conference on Computer Science & Education (ICCSE 2013)*. Colombo: IEEE, pp. 561–566.

177. Nakanishi, I., Ozaki, K. and Li, S. (2012) ‘Evaluation of the brain wave as biometrics in a simulated driving environment’, in *The International Conference of the Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG* -. Darmstadt: IEEE, pp. 1–5.

178. Nanavati, S., Thieme, M. and Nanavati, R. (2002) *Biometrics Identity Verification in a Networked World*. Edited by M. Eldridge and A. Obi. New York: Robert Ipsen.

179. National Science and Technology Council NSTC (2014) *Biometrics.gov - Introduction to Biometrics*. Available at: http://www.biometrics.gov/ReferenceRoom/Introduction.aspx (Accessed: 30 September 2014).

180. Niinuma, K., Park, U. and Jain, A. (2010) ‘Soft biometric traits for continuous user authentication’, *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 5(4), pp. 771–780.

181. NIST (2008) *NIST/ITL Conformance Test Suite for Patron Format A Data Structures Speci-fied in ANSI INCITS , Common Biometric Exchange Formats Framework (CBEFF)*.

182. NIST (2014a) *Face Recognition Grand Challenge (FRGC)*. Available at: http://www.nist.gov/itl/iad/ig/frgc.cfm (Accessed: 1 October 2014).

183. NIST (2014b) *Face Recogntion Vendor Test (FRVT) 2000*. Available at: http://www.nist.gov/itl/iad/ig/frvt-2000.cfm (Accessed: 1 October 2014).

184. NSTC (2005) *Biometrics: History*, *Subcommittee on Biometrics, National Science and Technology Council*. Available at: www.biometrics.gov (Accessed: 1 October 2014).

185. NSTC (2006a) ‘Biometrics “ Foundation Documents ”’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–166.

186. NSTC (2006b) ‘Biometrics Glossary’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–33.

187. NSTC (2006c) ‘Biometrics Overview’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–10.

188. NSTC (2006d) ‘Dynamic Signature’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–7.

189. NSTC (2006e) ‘Face Recognition’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–10.

190. NSTC (2006f) ‘Iris Recognition’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–10.

191. NSTC (2006g) ‘Palm Print Recognition’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–10.

192. NSTC (2006h) ‘Speaker Recognition’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–9.

193. NSTC (2006i) ‘Vascular Pattern Recognition’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–6.

194. NSTC (2011a) ‘Biometrics Technology and Standards Overview’, *Subcommittee on Biometrics, National Science and Technology Council*, pp. 1–72. doi: 10.1007/SpringerReference_132.

195. NSTC (2011b) ‘The National Biometrics Challenge’, *National Science and Technology Council Subcommittee on Biometrics and Identity Management*.

196. O’Gorman, L. (2003) ‘Comparing passwords, tokens, and biometrics for user authentication’, *Proceedings of the IEEE*, 91(12), pp. 2021–2040. doi: 10.1109/JPROC.2003.819611.

197. Ojala, S., Keinanen, J. and Skytta, J. (2008) ‘Wearable Authentication Device for Transparent Login in Nomadic Applications Environment’, in *2nd International Conference on Signals, Circuits and Systems*, pp. 1–6.

198. Onyesolu, M., Ejiofor, V., Onyeizu, M. and Ugoh, D. (2013) ‘Enhancing Security in a Distributed Examination Using Biometrics and Distributed Firewall System’, *International Journal of Emerging Technology and Advanced Engineering*, 3(9), p. 6.

199. Oracle (2016) *Oracle*. Available at: http://www.oracle.com/technetwork/java/index.html (Accessed: 5 October 2016).

200. Pan, C., Yang, K. and Lee, T. (2004) ‘Secure Online Examination Architecture Based on Distributed Firewall’, in *IEEE International Conference on e-Technology, e-Commerce and e-Service*. Ieee, pp. 533–536. doi: 10.1109/EEE.2004.1287359.

201. Percival, N., Percival, J. and Martin, C. (2008) ‘The Virtual Invigilator: A Network-based Security System for Technology-enhanced Assessments’, in *the World Congress on Engineering and Computer Science*. San Francisco, p. 6.

202. Phillips, J., Scruggs, T., O’Toole, A., Flynn, P., Bowyer, W., Schott, C., Sharpe, M. (2009) ‘FRVT 2006 and ICE 2006 Large-Scale Experimental Results’, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(5), pp. 831–846.

203. Pleva, M., Bours, P. and Hladek, D. (2016) ‘Using current biometrics technologies for authentication in e-learning assessment’, in *International Conference on Emerging eLearning Technologies and Applications (ICETA)*.

204. Podio, F. (2011) ‘Published International Biometric Standards Developed’, *by ISO/IEC JTC 1/SC 37 – Biometrics and Adopted by INCITS as INCITS/ISO/IEC Standards*, pp. 1–16.

205. Porta, M., Ricotti, S. and Perez, C. (2012) ‘Emotional e-learning through eye tracking’, in *IEEE Global Engineering Education Conference (EDUCON)*. Marrakech: IEEE, pp. 1–6. doi: 10.1109/EDUCON.2012.6201145.

206. Prakash, L. and Saini, D. (2012) ‘E-assessment for e-learning’, in *Engineering Education: Innovative …*. Kottayam: IEEE, pp. 1–6.

207. Przybocki, M., Martin, A. and Le, A. (2007) ‘Speaker recognition evaluations utilising the mixer corpora – 2004, 2005, 2006’, . *IEEE Trans. Audio Speech Lang. Process*, 15(7), pp. 1951–1959.

208. Pusara, M. and Brodley, C. (2004) 'User re-authentication via mouse movements', in *In Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*. Washington DC, USA, pp. 1–8.

209. Rabuzin, K., Baca, M. and Sajko, M. (2006) 'E-learning: Biometrics as a Security Factor', in *International Multi-Conference on Computing in the Global Information Technology, 2006. ICCGI '06.* Bucharest: IEEE, p. 64. doi: 10.1109/ICCGI.2006.28.

210. Ratha, N. K. and Govindaraju, V. (2008) *Advances in Biometrics: Sensors, Algorithms and Systems*, *Communications of the ACM*. Edited by N. K. Ratha and V. Govindaraju. New York: Springer-Verlag London Limited. doi: 10.1145/328236.328110.

211. Respondus (2014) *Real People. Real Proctoring. - Online Proctoring - ProctorU*. Available at: http://www.proctoru.com/ (Accessed: 21 October 2014).

212. Rigas, I. and Komogortsev, O. V (2014) 'Biometric Recognition via Probabilistic Spatial Projection of Eye Movement Trajectories in Dynamic Visual Environments', 9(10), pp. 1743–1754.

213. Rogers, C., Witt, A. and Solomon, A. (2015) *An Identification System for Head Mounted Displays*. Worcester Polytechnic Institute.

214. Rosen, W. a. and Carr, M. E. (2013) 'An autonomous articulating desktop robot for proctoring remote online examinations', in *2013 IEEE Frontiers in Education Conference,*. Oklahoma City, OK: Ieee, pp. 1935–1939. doi: 10.1109/FIE.2013.6685172.

215. Ross, A. (2011) 'Advances in Ear Biometrics', in *Presentation at West Virginia University*, pp. 1–34.

216. Ross, A. and Jain, A. (2003) 'Information fusion in biometrics', *Pattern Recognition Letters*, 24(13), pp. 2115–2125. doi: 10.1016/S0167-8655(03)00079-5.

217. Roth, J., Liu, X., Ross, A. and Metaxas, D. (2013) 'Biometric authentication via keystroke sound', in *International Conference on Biometrics (ICB)*. Madrid: IEEE. doi: 10.1109/ICB.2013.6613015.

218. Rovai, A. (2000) 'Online and traditional assessments: what is the difference?', *The Internet and Higher Education*, 3(2000), pp. 141–151.

219. Rowe, N. (2004) 'Cheating in online student assessment: Beyond plagiarism', *Online Journal of Distance Learning Administration*. Available at: http://www.westga.edu/~distance/ojdla/summer72/rowe72.html (Accessed: 1 October 2014).

220. Roy, S. and Biswas, A. (2011) 'A Personal Biometric Identification Technique based on Iris Recognition', *(IJCSIT) International Journal of Computer Science and Information Technologies*, 2(4), pp. 1474–1477.

221. Sabbah, Y., Saroit, I. and Kotb, A. (2012) 'A Smart Approach for Bimodal Biometric Authentication in Home-Exams (SABBAH Model)', *Biometrics and Bioinformatics*. Cairo, p. 13.

222. Sabbah, Y., Saroit, I. and Kotb, A. (2012) 'Synchronous Authentication with Bimodal Biometrics for e-Assessment', in *2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*. Giza, pp. 17–18.

223. Sabbah, Y. W. S. (2012) *Proposed Models for Secure E-Examination System*. Cairo University.

224. Sae-bae, N., Memon, N., Isbister, K. and Ahmed, K. (2014) 'Multi-touch Gesture Based Authentication', *IEEE Transactions on Information Forensics and Security*, 6013. doi: 10.1109/TIFS.2014.2302582.

225. Saeed, U. (2015) 'Eye movements during scene understanding for biometric identification', *Pattern Recognition Letters*. Elsevier Ltd., 0, pp. 1–6. doi: 10.1016/j.patrec.2015.06.019.

226. Saevanee, H. (2014) *Continuous User Authentication Using Multi-Modal Biometrics*. Plymouth University.

227. Saevanee, H., Clarke, N. and Furnell, S. (2012) 'Multi-Modal Behavioural Biometric Authentication for Mobile Devices', in *27th IFIP International Information Security and Privacy Confer-ence (SEC2012)*, pp. 465–474.

228. Sang-Kyun Im, Hyung-Man Park, Soo-Won Kim, Chang-Kyung Chung, H.-S. C. (2000) 'Improved vein pattern extracting algorithm and its implementation', in *International Conference on Consumer Electronics, 2000. ICCE. 2000 Digest of Technical Papers.* Los Angles: IEEE, pp. 2–3.

229. Sayed, B. and Traore, I. (2013) 'Biometric authentication using mouse gesture dynamics', *IEEE Systems Journal*, 7(2), pp. 262–274.

230. Shaver, C. D. and Acken, J. M. (2010) 'Effects of equipment variation on speaker recognition error rates', in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*. Dallas: Ieee, pp. 1814–1817. doi: 10.1109/ICASSP.2010.5495401.

231. Shen, C., Cai, Z. and Guan, X. (2012) 'Continuous authentication for mouse dynamics: A pattern-growth approach', in *International Conference on Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP*. Boston: IEEE.

232. Shen, C., Cai, Z. and Guan, X. (2013) 'User authentication through mouse dynamics', *IEEE TTransactions on Information Forensics and Security*, 8(1), pp. 16–30.

233. Shu, W. and Zhang, D. (1998) 'Automated personal identification by palmprint', *Optical Engineering*. Available at: http://ac.els-cdn.com/S0031320302000304/1-s2.0-S0031320302000304-main.pdf?_tid=d59a07b4-4a26-11e4-8761-00000aab0f6b&acdnat=1412249318_872435d81cfd2c88f9817ace1bd6f9e2 (Accessed: 6 November 2014).

234. Sim, T., Zhang, S., Member, S., Janakiraman, R. and Kumar, S. (2007) 'Continuous Verification Using Multimodal Biometrics', 29(4), pp. 687–700.

235. Socolinsky, D. A., Wolff, L. B., Neuheisel, J. D., Eveland, C. K. and Street, W. (2003) 'Illumination Invariant Face Recognition Using Thermal Infrared Imagery', *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001. CVPR 2001.*, 1, p. I-534.

236. Socolinsky, D. and Selinger, A. (2004) 'Thermal face recognition in an operational scenario', in *the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04)*. IEEE, pp. 1012–1019. doi: 10.1109/CVPR.2004.1315275.

237. Software Secure (2008) *Remote-Proctor-Now for Educational Institutions*. Available at: http://samevaglobal.com/wp-content/uploads/2014/06/Remote-Proctor-NOW-Data-Sheet-EDU.pdf.

238. Software Secure (2011) *Online and traditional assessments: what is the difference?*, *The Internet and Higher Education*. London: Springer London. doi: 10.1007/978-1-84628-609-4.

239. Software Secure (2013) *Watchful Eyes: A Comparative Look at Online Test Proctoring Models*, *A White Paper from Software Secure, Inc.* London.

240. Software Secure (2017) *Remote Proctor Solutions | Proctor Exam | Software Secure*. Available at: http://www.softwaresecure.com/products-overview/ (Accessed: 15 June 2017).

241. Soltane, M., Doghmane, N. and Guersi, N. (2010) 'Face and Speech Based Multi-Modal Bio-metric Authentication', *International Journal of Advanced Science and Technology*, 21(6), pp. 41–56.

242. Sourcebook (2014) *The History of Fingerprints*. Available at: http://onin.com/fp/fphistory.html (Accessed: 1 October 2014).

243. Sreekala, P., Jose, V., Joseph, J. and Joseph, S. (2012) 'The human iris structure and its application in security system of car', *AICERA 2012 - Annual International Conference on Emerging Research Areas: Innovative Practices and Future Trends*. doi: 10.1109/AICERA.2012.6306710.

244. Stanić, M. (2013) 'Continuous User Verification Based on Behavioral Biometrics Using Mouse Dynamics', in *Proceedings of the ITI 2013 35th Int. Conf. on Information Technology Interfaces*. Cavtat, Croatia. doi: 10.2498/iti.2013.0505.

245. Stolfo, S.J., Wei F., Wenke L., Prodromidis, A., Chan, P. K. (2000) 'Cost-based modeling for fraud and intrusion detection', *Information Survivability Conference and Exposition*.

246. Stuber-McEwen, D., Wiseley, P. and Hoggatt, S. (2009) 'Point, click, and cheat: Frequency and type of academic dishonesty in the virtual classroom', *Online Journal of Distance Learning Administration*, XII(III). Available at: http://www.westga.edu/~distance/ojdla/fall123/stuber123.html (Accessed: 1 October 2014).

247. Sudarvizhi, S. and Sumathi, S. (2013) 'A Review on Continuous Authentication Using Multimodal Biometrics', *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, 3(1), pp. 192–196.

248. Sulong, A. and Siddiqi, M. U. (2009) 'Intelligent keystroke pressure-based typing biometrics authentication system using radial basis function network', in *2009 5th International Colloquium on Signal Processing & Its Applications*. Kuala Lumpur: Ieee, pp. 151–155. doi: 10.1109/CSPA.2009.5069206.

249. Sumathi, D. (2010) 'E-learning and pedagogical challenges', in *Distance Learning and Education (ICDLE), 2010 4th International Conference on*. San Juan: IEEE, pp. 112–114.

250. Tang, Y., Sun, X., Huang, D., Morvan, J., Wang, Y. and Chen, L. (2015) '3D Face Recognition with Asymptotic Cones based Principal Curvatures', pp. 466–472.

251. Tayal, A. (2009) 'A multimodal biometric system coupling iris recognition and speaker identification systems through decision theory', in *2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*. Hong Kong: Ieee, pp. 135–137. doi: 10.1109/ICASID.2009.5276939.

252. Tayal, A. and Balasubramaniam, R. (2009) 'A multimodal biometric authentication system using decision theory, iris and speech recognition', in *2nd International Workshop on Nonlinear Dynamics and Synchronization, 2009. INDS '09*. Klagenfurt: IEEE.

253. Teh, P. S., Teoh, A. B. J., Tee, C. and Ong, T. S. (2010) 'Keystroke dynamics in password authentication enhancement', *Expert Systems with Applications*. Elsevier Ltd, 37(12), pp. 8618–8627. doi: 10.1016/j.eswa.2010.06.097.

254. The Open University (2016) *TeSLA Project*. Available at: http://tesla-project.eu/tesla-technical-architecture/ (Accessed: 1 January 2016).

255. Times Newspapers (2007) *How quickly did you type that password?* Available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article1667057.ece (Accessed: 24 May 2015).

256. Toshiba America Information Systems (2001) *Face recognition*. Available at: http://us.toshiba.com/computers/research-center/technology-guides/face-recognition (Accessed: 20 January 2015).

257. Traoré, I. and Ahmed, A. A. E. (2012) *Continuous Authentication Using Biometrics: Data, Models, and Metrics*. PA, USA: IGI Global.

258. Tsai, P., Khan, M., Pan, J. and Liao, B. (2014) 'Interactive Artificial Bee Colony Supported Pas-sive Continuous Authentication System', *IEEE SYSTEMS JOURNAL, IEEE Biometrics Compendium*, 8(2), pp. 395–405.

259. Tsalakanidou, F., Malassiotis, S. and Strintzis, M. G. (2007) 'A 3D face and hand biometric system for robust user-friendly authentication', *Pattern Recognition Letters*, 28(16), pp. 2238–2249. doi: 10.1016/j.patrec.2007.07.005.

260. UKBA (2011) *Using the iris recognition immigration system (IRIS)*. Available at: http://webarchive.nationalarchives.gov.uk/20140110181512/http://www.ukba.homeoffice.gov.uk/customs-travel/Enteringtheuk/usingiris/howenterwithiris/ (Accessed: 3 February 2014).

261. Ullah, A., Xiao, H. and Lilley, M. (2012) 'Profile based student authentication in online examination', in *International Conference on Information Society (i-Society)*. London: IEEE, pp. 109–113.

262. University, M. S. (2016) *Online Test Proctoring*. Available at: https://outreach.missouristate.edu/online/testproctoring.htm (Accessed: 1 January 2016).

263. USMA (2012) *Biometrics Metrics Report v3.0*.

264. Vallabhu, H. and Satyanarayana, R. (2012) 'Biometric Authentication as a Service on Cloud: Novel Solution', *International Journal of Soft Computing and Engineering*, 2(4), pp. 163–165.

265. Weaver, A. C. (2006) 'Biometric Authentication', *Computer*, 39(2), pp. 96–97. doi: 10.1109/MC.2006.47.

266. Wei, L., Cong, Z. and Zhiwei, Y. (2010) 'Fingerprint Based Identity Authentication for Online Examination System', in *2010 Second International Workshop on Education Technology and Computer Science*. Wuhan: Ieee, pp. 307–310. doi: 10.1109/ETCS.2010.409.

267. Willems, C. and Meinel, C. (2012) 'Online assessment for hands-on cyber security training in a virtual lab', in *Proceedings of the 2012 IEEE Global Engineering Education*

Conference (EDUCON). Marrakech: Ieee, pp. 1–10. doi: 10.1109/EDUCON.2012.6201149.

268. Wood (1977) 'The use of passwords for controlling access to remote computer systems and services', in *Proceedings of the June 13-16, 1977, national computer conference on (AFIPS '77)*. New York, USA: ACM Press, pp. 27–33.

269. Woodward, J. D. J., Orlans, N. M. and Higgins, P. T. (2003) *Biometrics: Identity Assurance in the Information Age*. New York: McGraw Hill/Osborne.

270. Wu, R. (2011) 'Ears: The New Fingerprints?', *Yale Scientific Magazine*.

271. Yeung (2004) 'First international signature verification competition'.

272. Yiran, S., Wen, H. and Mingrui, Y. (2014) 'Face recognition on smartphones via optimised Sparse Representation Classification', in *Proceedings of the 13th International Symposium on Information Processing in Sensor Networks, IPSN-14*.

273. York, U. of (2014) *Guide to Assessment, Standards, Marking and Feedback 2013–2014*. York.

274. Yu, X., Gao, Y. and Zhou, J. (2014) 'Face Recognition Using 3D Directional Corner Points', *2014 22nd International Conference on Pattern Recognition*, pp. 2802–2807. doi: 10.1109/ICPR.2014.483.

275. Zafeiriou, S. and Pantic, M. (2011) 'Facial Behaviometrics: the Case of Facial Deformation in Spontaneous Smile / Laughter University of Twente', in *2011 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW),*. Colorado Springs, CO: IEEE, pp. 13–19.

276. Zhang, Y., Ma, Z. and He, Y. (2012) 'A high-speed iris recognition system based on DM6446', *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, pp. 1518–1522. doi: 10.1109/CECNet.2012.6201575.

277. Zhao, Q. and Ye, M. (2010) 'The application and implementation of face recognition in authentication system for distance education', in *Networking and Digital Society (ICNDS)*. Wenzhou: IEEE, pp. 487–489.

278. Zhu, J., Hu, H., Hu, S., Wu, P. and Zhang, J. Y. (2013) 'Mobile Behaviometrics: Models and applications', in *2013 IEEE/CIC International Conference on Communications in China (ICCC)*. Xi'an: Ieee, pp. 117–123. doi: 10.1109/ICCChina.2013.6671100.

Appendices

Appendix A: Approval Forms and Ethical Approval Notifications

Appendix B: Publications

Appendix F (Electronic): Eye Tracker Calibration/Re-Calibration

Appendix C (Electronic): Evaluation Questionnaires

Appendix D (Electronic): Experts' and Academics' Interviews

Appendix E (Electronic): Students Interviews

Appendix A: Approval Forms and Ethical Approval Notifications

- **E-Invigilation of E-Assessment – An Experiment**

RESEARCH WITH PLYMOUTH UNIVERSITY

17 February 2016

CONFIDENTIAL
Salam Ketab
School of Computing, Electronics and Mathematics

Dear Salam

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

E-Invigilation of E-Assessment – An Experiment

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Nathan Clarke
Dr Paul Dowland

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

T +44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Christine Mushens BA
Faculty Business Manager

PLYMOUTH UNIVERSITY FACULTY OF SCIENCE AND ENVIRONMENT

Research Ethics Committee

APPLICATION FOR ETHICAL APPROVAL OF RESEARCH INVOLVING

HUMAN PARTICIPANTS

All applicants should read the guidelines which are available via the following link:

https://staff.plymouth.ac.uk//SciEnv/humanethics/intranet.htm

This is a WORD document. Please complete in WORD and extend space where necessary.

*All applications must be word processed. Handwritten applications **will** be returned.*

Please submit with interview schedules and/or questionnaires appropriately.

Postgraduate and Staff must submit a signed copy to SciEnvHumanEthics@plymouth.ac.uk

Undergraduate students should contact their School Representative of the Science and Environment Research Ethics Committee or dissertation advisor prior to completing this form to confirm the process within their School.

---

1. TYPE OF PROJECT

1.1 What is the type of project? (Tick 1 only)

STAFF should tick one of the three options below:

Specific project ☐

Thematic programme of research ☐

Practical / Laboratory Class ☐

1.2 Tick 1 only

POSTGRADUATE STUDENTS should tick one of the options below:

Taught Masters Project ☐

M.Phil / PhD by research ☑

UNDERGRADUATE STUDENTS should tick one of the two options below:

Student research project ☐

Practical / Laboratory class where you are acting as the experimenter ☐

2. APPLICATION

2.1 TITLE of Research project
E-Invigilation of E-Assessment – An Experiment
2.2 General summary of the proposed research for which ethical clearance is sought, briefly outlining the aims and objectives and providing details of interventions/procedures involving participants (no jargon)
This experiment is being conducted to explore the feasibility of monitoring students while taking university online assessments. The experiment will focus upon continuous authentication through 2D and 3D facial recognition using a front-facing peripheral 3D camera (F200, Windows Platform). In addition to capturing facial images, the software will also capture the session using a microphone and use eye tracking technology to follow and record the participant eye movement. The eye tracking is linked to camera to take a picture whenever the student moves his/her eyes away from the screen for a period of time. This project involves participants of 18 years and older to take a completely controlled/monitored exam for a maximum of 15 minutes. In addition, the collected data will be treated anonymously.
2.3 Physical site(s) where research will be carried out
The research will be conducted within Centre for Security, Communications and Network Research (CSCAN) at Plymouth University.
2.4 External Institutions involved in the research (e.g. other university, hospital, prison etc.)
N/A
2.5 Name, telephone number, e-mail address and position of lead person for this project (plus full details of Project Supervisor if applicable)
1- Salam Ketab (Research student) – salam.ketab@plymouth.ac.uk, +441752586287 2- Prof. Nathan Clarke (Director of study) – N.Clarke@plymouth.ac.uk, +441752586226 3- Dr. Paul Dowland (Second Supervisor) - P.Dowland@plymouth.ac.uk, +441752586226
2.6 Start and end date for research for which ethical clearance is sought (NB maximum period is 3 years)
Start date: February 2016 **End date: April 2016**
2.7 Has this same project received ethical approval from another Ethics Committee?
No ☑ **Yes** ☐

2.8 If yes, do you want Chairman's action?
No ☑ **Yes** ☐
If yes, please include other application and approval letter and STOP HERE. If no, please continue

3. PROCEDURE

3.1 Describe procedures that participants will engage in, Please do not use jargon
The experiment will be conducted in the Centre for Security, Communications and Network Research (CSCAN) office at Plymouth University on a dedicated computer equipped with the required technologies to accomplish the experiment objectives. The purpose of that experiment is to collect the biometric data, to investigate the feasibility of the suggested technologies to detect any cheating attempt. The capturing devices will be attached to a computer in front of the participant (the front-facing peripheral F200 3D camera and The Eye Tribe eye tracker). Taking into consideration the optimum distance of the user's eyes from the computer screen, and for participants convenience and to avoid high error of the depth measurements, the participant's face will be posed in front of the computer screen within 40 to 76 centimetres away from the acquisition devices. Participants will not need to do anything but merely taking a virtual assessment (online IQ test for e-assessment simulation) that contains simple questions for a maximum of 15 minutes. During the experiment, the participants' biometrics/data (2D, 3D, depth, and infrared images) and eye movement or focus on the screen will be collected using custom software for that purpose via a 3D web camera and Eye Tracker sensor then saved anonymously in a secure database. All of the information will be treated confidentially and data will be anonymous during the collection, storage and publication of research material. Participants will be asked to accept their consent before they can proceed with the experiment. For this project, the participants should be 18 years or older. They are free to withdraw up until the end of the experiment (end of the exam simulation). A number of participants will be asked to do some set of tasks to exploit a set of predefined threat factors, such as: - Pretending to be the genuine exam taker. - Looking outside the screen for periods of time. - Zero, two or more participant faces looking at the screen in specific time. - Turning face left, right, up and down for specific time. - Speaking during the test time (including answering the questions by somebody else). - Increasing or decreasing the face distance from the screen. As part of the experiment scenario, the participant should follow some simple instructions that will be given by the investigator. Once participants have completed the simulated exam, they will press the Exit Test button and all information will be held securely within the dedicated computer database. If users would like to be notified of the overall findings from the experiment study, they will be provided with the contact e-mail address of the researcher.
3.2 How long will the procedures take? Give details
The total amount of time needed for each participant will range between 10 to 15 minutes depending on their knowledge about the questions in a virtual/simulated assessment. The task will

last no more than 15 minutes.
3.3 Does your research involve deception?
No ☑ **Yes** ☐
3.4 If yes, please explain why the following conditions apply to your research: N/A
a) Deception is completely unavoidable if the purpose of the research is to be met
N/A
b) The research objective has strong scientific merit
N/A
c) Any potential harm arising from the proposed deception can be effectively neutralised or reversed by the proposed debriefing procedures (see section below)
N/A
3.5 Describe how you will debrief your participants
At the beginning of the experiment, all participants will be briefed and invited to ask any questions regarding the experiment. After the experiment, participants are free to ask any further questions.
3.6 Are there any ethical issues (e.g. sensitive material)?
No ☑ **Yes** ☐
3.7 If yes, please explain. You may be asked to provide ethically sensitive material. See also section 11
N/A

4. BREAKDOWN OF PARTICIPANTS

4.1 Summary of participants

Type of participant	*Number of participants*
Non-vulnerable Adults	***Approximately 30***
Minors (< 16 years)	***N/A***
Minors (16-18 years)	***N/A***
Vulnerable Participants (other than by virtue of being a minor)	***N/A***
	N/A

Other (please specify)	
TOTAL	***Minimum 30***

4.2 How were the sample sizes determined?
As the experiment will be implemented on the Communications and Network Research (CSCAN) office at Plymouth University, with the dedicated experiment time in mind, the participants will be PhD researches in Centre for Security, Communications and Network Research (CSCAN) (the most targeted), other Plymouth University postgraduate or undergraduate students, I would expect approximate target of participants to be 30 students in order to facilitate a meaningful analysis. 30 participants will be considered sufficient baseline since some other researches have been conducted using the same sample size.
4.3 How will subjects be recruited?
The subjects will be recruited via e-mail or directly, predominantly targeting colleagues and staff in the School of Computing, Electronics and Mathematics (Faculty of Science and Engineering) and other researchers or students in Plymouth University.
4.4 Will subjects be financially rewarded? If yes, please give details.
No

5. NON-VULNERABLE ADULTS

5.1 Are some or all of the participants non-vulnerable adults?
No ☐ **Yes** ✓ ☐
5.2 Inclusion / exclusion criteria
Participants who are 18 years old and above, agree and understand all procedure able to take part in this study.
5.3 How will participants give informed consent?
The participants will be given the consent at the beginning of the study, should they wish to carry out the study, ensuring their understand that they can withdraw from the experiment at any time up until the end of their participation. Please note that there is no possibility of involving any participant below 18 years old.
5.4 Consent form(s) attached
No ☐ **Yes** ☑ ✓
If no, why not?
N/A
5.5 Information sheet(s) attached
✓

No ☐ **Yes** ☐
If no, why not?
N/A
5.6 How will participants be made aware of their right to withdraw at any time?
Participants will have the right to withdraw at any stage up to the completion of the data collection process. Should any participant to withdraw from the study, their data will be securely removed from the data storage and completely destroyed.
5.7 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?
Participants will be informed that their data will be anonymous, securely stored and only used for the purpose stated in the briefing. In accordance with Plymouth University guidelines, the data will be stored for ten years. Once the ten-year time period is reached, the data will be securely destroyed.

6. MINORS <16 YEARS

6.1 Are some or all of the participants under the age of 16?
No ☑ **Yes** ☐
If yes, please consult special guidelines for working with minors. If no, please continue.
6.2 Age range(s) of minors
N/A
6.3 Inclusion / exclusion criteria
N/A
6.4 How will minors give informed consent? Please tick appropriate box and explain (See guidelines)
N/A **Opt-in** ☐ **Opt-out** ☐
6.5 Consent form(s) for minor attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
6.6 Information sheet(s) for minor attached

N/A	**No** ☐	**Yes** ☐
If no, why not?		
N/A		
6.7 Consent form(s) for parent / legal guardian attached		
N/A	**No** ☐	**Yes** ☐
If no, why not?		
N/A		
6.8 Information sheet(s) for parent / legal guardian attached		
N/A	**No** ☐	**Yes** ☐
If no, why not?		
N/A		
6.9 How will minors be made aware of their right to withdraw at any time?		
N/A		
6.10 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?		
N/A		

7. MINORS 16-18 YEARS OLD

7.1 Are some or all of the participants between the ages of 16 and 18?		
	No ☑	**Yes** ☐
If yes, please consult special guidelines for working with minors. If no, please continue.		
7.2 Inclusion / exclusion criteria		
N/A		
7.3 How will minors give informed consent? (See guidelines)		
N/A		
7.4 Consent form(s) for minor attached		

N/A	**No** ☐	**Yes** ☐
If no, why not?		
N/A		
7.5 Information sheet(s) for minor attached		
N/A	**No** ☐	**Yes** ☐
If no, why not?		
N/A		
7.6 Consent form(s) for parent / legal guardian attached		
N/A	**No** ☐	**Yes** ☐
If no, why not?		
N/A		
7.7 Information sheet(s) for parent / legal guardian attached		
N/A	**No** ☐	**Yes** ☐
If no, why not?		
N/A		
7.8 How will minors be made aware of their right to withdraw at any time?		
N/A		
7.9 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?		
N/A		

8. VULNERABLE GROUPS

8.1 Are some or all of the participants vulnerable? (See guidelines)		
	No ☑	**Yes** ☐
If yes, please consult special guidelines for working with vulnerable groups. If no, please continue.		

8.2 Describe vulnerability (apart from possibly being a minor)
N/A
8.3 Inclusion / exclusion criteria
N/A
8.4 How will participants give informed consent?
N/A
8.5 Consent form(s) for vulnerable person attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
8.6 Information sheet(s) for vulnerable person attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
8.7 Consent form(s) for parent / legal guardian attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
8.8 Information sheet(s) for parent / legal guardian attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
8.9 How will participants be made aware of their right to withdraw at any time?
N/A
8.10 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?

N/A

9. EXTERNAL CLEARANCES

Investigators working with children and vulnerable adults legally require clearance from the Disclosure and Barring Service (DBS)

9.1 Do ALL experimenters in contact with children and vulnerable adults have <u>current</u> DBS clearance? Please include photocopies.
No ☐ **Yes** ☐ **N/A** ☑
If no, explain
N/A
9.2 If your research involves external institutions (school, social service, prison, hospital etc) please provide cover letter(s) from institutional heads permitting you to carry out research on their clients, and where applicable, on their site(s). Are these included?
No ☐ **Yes** ☐ **N/A** ☑
If not, why not?

10. PHYSICAL RISK ASSESSMENT

10.1 Will participants be at risk of physical harm (e.g. from electrodes, other equipment)? (See guidelines)
No ☑ **Yes** ☐
10.2 If yes, please describe
N/A
10.3 What measures have been taken to minimise risk? Include risk assessment proformas.
N/A
10.4 How will you handle participants who appear to have been harmed?
N/A

11. PSYCHOLOGICAL RISK ASSESSMENT

11.1 Will participants be at risk of psychological harm (e.g. viewing explicit or emotionally sensitive material, being stressed, recounting traumatic events)? (See guidelines)
No ☑ **Yes** ☐

11.2 If yes, please describe
N/A
11.3 What measures have been taken to minimise risk?
N/A
11.4 How will you handle participants who appear to have been harmed?
N/A

12. RESEARCH OVER THE INTERNET

12.1 Will research be carried out over the internet?
No ☐✓ **Yes** ☐
12.2 If yes, please explain protocol in detail, explaining how informed consent will be given, right to withdraw maintained, and confidentiality maintained. Give details of how you will guard against abuse by participants or others (see guidelines)
N/A

13. CONFLICTS OF INTEREST & THIRD PARTY INTERESTS

13.1 Do any of the experimenters have a conflict of interest? (See guidelines)
No ☑ **Yes** ☐
13.2 If yes, please describe
N/A
13.3 Are there any third parties involved? (See guidelines)
No ☑ **Yes** ☐
13.4 If yes, please describe
N/A
13.5 Do any of the third parties have a conflict of interest?
No ☑ **Yes** ☐
13.6 If yes, please describe
N/A

14. ADDITIONAL INFORMATION

14.1 [Optional] Give details of any professional bodies whose ethical policies apply to this research
N/A
14.2 [Optional] Please give any additional information that you wish to be considered in this application
N/A

15. ETHICAL PROTOCOL & DECLARATION

To the best of our knowledge and belief, this research conforms to the ethical principles laid down by the University of Plymouth and by any professional body specified in section 14 above.

This research conforms to the University's Ethical Principles for Research Involving Human Participants with regard to openness and honesty, protection from harm, right to withdraw, debriefing, confidentiality, and informed consent

Sign below where appropriate:
STAFF / RESEARCH POSTGRADUATES

	Print Name	**Signature**	**Date**
Principal Investigator:	Salam Ketab	_____	15/12/2015
	Prof. Nathan Clarke	_____	15/12/2015
	Dr. Paul Dowland	_____	15/12/2015

Staff and Research Postgraduates should email the completed and signed copy of this form to Paula Simson.

UG Students

	Print Name	**Signature**	**Date**
Student:	_____	_____	_____
Supervisor / Advisor:	_____	_____	_____

Undergraduate students should pass on the completed and signed copy of this form to their School Representative on the Science and Environment Human Ethics Committee.

	Signature	**Date**
School Representative on Science and Environment Faculty Human Ethics Committee	_____	_____

Faculty of Science and Environment Research Ethics Committee List of School Representatives

School of Geography, Earth and Environmental Sciences	Dr Sanzidur Rahman
School of Biological Sciences	Dr Victor Kuri
School of Biomedical and Healthcare Sciences	Dr David J Price
School of Marine Science & Engineering	Dr Emily Beaumont (Chair)
	Dr Liz Hodgkinson
School of Computing & Mathematics	Mr Martin Beck
	Dr Mark Dixon
External Representative	Prof Linda La Velle
Lay Member	Rev. David Evans

Committee Secretary: Mrs Paula Simson
email: paula.simson@plymouth.ac.uk
tel: 01752 584503

SAMPLE SELF-CONSENT FORM
PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENVIRONMENT

Human Ethics Committee Sample Consent Form

CONSENT TO PARICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Salam Ketab

Title of Research

E-Invigilation of E-Assessment – An expermint

Brief statement of purpose of work

E-learning and particularly distance-based learning is becoming an increasingly important mechanism for education. Whilst a range of Virtual Learning Environments (VLEs) now exist to facilitate this, there are some significant limitations when considering the assessment options that are available. The lack of being able to provide invigilation in a remote-mode has restricted the types of assessments, with exams or in-class test assessments proving difficult to validate.

This study seeks to research and develop an e-invigilator that will provide continuous and transparent invigilation of the individual undertaking an electronic based exam or test.

The study will also seek to determine if the collected data using the suggested 3D camera and Eye Tracker are feasible to be employed to achieve transparent and continuous authentication within the online assessment environment.

As a participant, you will merely take a virtual online IQ test to simulate e-assessment for a maximum of 15 minutes, while the custom software collects your biometrics/data/pictures (e.g. 2D, 3D, depth, and infrared images). In addition to capturing facial images, the software will also capture the session using a microphone and use eye tracking technology to follow and record the your eye movement. The eye tracking is linked to camera to take a picture whenever you move your eyes away from the screen for a period of time. Based upon Plymouth University guidelines, collected data should be stored for ten years. Upon the completion of the ten-year period, the collected data will be securely destroyed.

At all stages of the study, confidentiality of the collected data and subsequent analysis will be maintained. At no time, will any identifying information about the participants be used in any publication or research output.

You have the right to withdraw at any stage upon until the completion of the data collection process. Should you wish to withdraw from the study, please contact Salam Ketab.

For information regarding the study, please contact:

Salam Ketab – salam.ketab@plymouth.ac.uk

For any questions concerning the ethical status of this study, please contact the secretary of the Human Ethics Committee – paula.simson@plymouth.ac.uk

---

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far

as possible, to avoid any risks, and that safety and health risks will have been

separately assessed by appropriate authorities (e.g. under COSHH regulations)

Under these circumstances, I agree to participate in the research.

Name: ……..

Signature: .....…….. Date: .....……..

SAMPLE INFORMATION SHEET FOR ADULT / CHILD

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENVIRONMENT

RESEARCH INFORMATION SHEET

Name of Principal Investigator

Salam Ketab

Title of Research

E-Invigilation of E-Assessment – An expermint

Aim of research

1- To monitor the exam taker and ensure that only allowed student is taking the exam, the experiment will focus upon continuous authentication through 2D and 3D facial recognition using a front-facing peripheral 3D camera (F200, Windows Platform).
2- To monitor and record the student eye movement. In addition, it aims to add more rules into client application such as checking the student distance from the screen or linking the camera with the eye tracker to take a picture whenever the student moves his/her eyes away from the screen for a period of time.
3- To record the surrounding sounds during the exam time.

Description of procedure

The capturing devices will be attached to a computer in front of the participant (the front-facing peripheral F200 3D camera and The Eye Tribe eye tracker). Taking into consideration the optimum distance of the user's eyes from the computer screen, and for participants convenience and to avoid high error of the depth measurements, the participant's face will be posed in front of the computer screen and within 40 to 76 centimetres away from the acquisition devices. Participants will not need to do anything but merely taking a virtual assessment (online IQ test for e-assessment simulation).

A number of participants will be asked to do some set of tasks to exploit a set of predefined threat factors, such as pretending to be the genuine exam taker.

Description of risks

All of the information will be treated confidentially and data will be anonymous during the collection, storage and publication of research material.

Benefits of proposed research

The lack of being able to provide invigilation in a remote-mode has restricted the types of assessments, with exams or in-class test assessments proving difficult to validate. This research seeks to research and develop an e-invigilator that will provide continuous and transparent invigilation of the individual undertaking an electronic based exam or test.

Right to withdraw

You have the right to withdraw at any stage. Your biometric and any recorded data will be removed and securely deleted. Also, declining participation and/or asking to withdraw from this study should not affect your PhD progression or your relationship with your supervisors where appropriate.

If you are dissatisfied with the way the research is conducted, please contact the principal investigator in the first instance: telephone number *[*01752 586287*]*. If you feel the problem has not been resolved please contact the secretary to the Faculty of Science and Environment Human Ethics Committee: Mrs Paula Simson 01752 584503.

- **E-Invigilation of E-Assessments Syetem Evaluation**

RESEARCH WITH PLYMOUTH UNIVERSITY

19 July 2016

CONFIDENTIAL
Salam Ketab
School of Computing, Electronics and Mathematics

Dear Salam

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

E-Invigilation of E-Assessments System Evaluation

I am pleased to inform you that this has been approved subject to the following recommendations/conditions:

- Section 3.1 - In the description of activity, it says all students will sign the form, an email from the students saying they agree to participate given the conditions might be easier to manage since the students may not be individually seen.
- Section 3.5 – what will happen after? Thank you and provide info? Can they retract the information provided at any time?
- In the questionnaire for students likert scale of concerned for Q 4 and 5 seems odd – perhaps just most to least without the concern? Likewise for questions 10-13.
- What is a 'spoofing action'?
- Please clarify where "experts", "academics", and "students" will be recruited from. Although some information is given in Section 4.3, it is not clear whether these will be recruited from within or outside the University.
- Revise information sheet and consent form to address the following items:
  - The information and consent forms could be confusing as they refer to different groups of people: Simplify for the potential volunteers to include text relevant only to their group

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

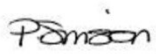
T +44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Christine Mushens BA
Faculty Business Manager

- While confidentiality is mentioned (with regards to final report), it is not clear how the recordings will be managed. If they will be destroyed (i.e. erased) after transcription or evaluation, This should be made explicit in the forms.
- Explain how long participation is expected: i.e. how many sessions, how long they will take.

I would be grateful if you could email your amended application to me for my records please.

Kind regards



Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Nathan Clarke
Dr Paul Dowland

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

T +44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Christine Mushens BA
Faculty Business Manager

PLYMOUTH UNIVERSITY FACULTY OF SCIENCE AND ENVIRONMENT

Research Ethics Committee

APPLICATION FOR ETHICAL APPROVAL OF RESEARCH INVOLVING

HUMAN PARTICIPANTS

All applicants should read the guidelines which are available via the following link:

https://staff.plymouth.ac.uk//SciEnv/humanethics/intranet.htm

This is a WORD document. Please complete in WORD and extend space where necessary.

*All applications must be word processed. Handwritten applications **will** be returned.*

Please submit with interview schedules and/or questionnaires appropriately.

Postgraduate and Staff must submit a signed copy to SciEnvHumanEthics@plymouth.ac.uk

Undergraduate students should contact their School Representative of the Science and Environment Research Ethics Committee or dissertation advisor prior to completing this form to confirm the process within their School.

---

4. TYPE OF PROJECT

1.1 What is the type of project? (Tick 1 only)

STAFF should tick one of the three options below:

Specific project ☐

Thematic programme of research ☐

Practical / Laboratory Class ☐

1.3 Tick 1 only

POSTGRADUATE STUDENTS should tick one of the options below:

Taught Masters Project ☐

M.Phil / PhD by research ☑

UNDERGRADUATE STUDENTS should tick one of the two options below:

Student research project ☐

Practical / Laboratory class where you are acting as the experimenter ☐

5. APPLICATION

2.1 TITLE of Research project
E-Invigilation of E-Assessments Syetem Evaluation
2.2 General summary of the proposed research for which ethical clearance is sought, briefly outlining the aims and objectives and providing details of interventions/procedures involving participants (no jargon)
The aim of this study is to research and develop a novel e-invigilator that will provide continuous and transparent invigilation of the individual undertaking an electronic based exam or test. Despite the promising validation results we obtained in a previous experiment of the research, there is a need for an additional qualitative and quantitative evaluation by stakeholders of the system. Following the development of the system, to evaluate all dimensions of the E-Invigilation of E-Assessments system (EIEA), there are three separate stakeholder (namely: experts, academics and students) will get three separate sets of information and three separate sets of questions, in two cases it is a qualitative-based survey and the other one is a quantitative-based and qualitative-based survey. • **Experts**: Experts with experience and a knowledge background in e-assessment are needed. Hence, an expert-based (qualitative-based survey) evaluation should take place with the aim of validating the novelty, reviewing the performance and identifying its limitations. Experts will be formally invited either in person or via e-mail. Once an expert initially accepted the invitation the consent form will be sent to him/her to sign. A summary of how the system works including screenshots of the interfaces will be also emailed to the expert prior to the interview. They will be then asked to suggest the time of conducting the interview. A demo of the system will be presented to the interviewee, then a set of open-ended questions will be asked. All sessions will be recorded after having a permission of the interviewees. • **Academics:** To prove the usability of the approach, the perspectives of the academics are also essential for additional qualitative evaluation (qualitative-based survey). They will be formally invited either in person or via e-mail. Once an academic initially accepted the invitation the consent form will be sent to him/her to sign. A summary of how the system works including screenshots of the interfaces will be also emailed to the academic prior to the interview. They will be then asked to suggest the time of conducting the interview. A demo of the system will be presented to the interviewee, then a

set of open-ended questions will be asked. All sessions will be recorded after having a permission of the interviewees.

- **Student:** To prove the usability and non-intrusiveness of the approach, the student point of view is also necessary to add quantitative and qualitative evaluation. They will be formally invited either in person or via e-mail. Once a student initially accepted the invitation the consent form will be sent to him/her to sign. A summary of how the system works including screenshots of the interfaces and a demo of the system will be also emailed to the student. In order to get their feedback, a set of questions will be sent to them via e-mail.

2.3 Physical site(s) where research will be carried out

In case of expert, the interview will be conducted over the internet (Skype interviews) or face-to-face at participants' locations. The questions will be asked directly.

In case of academic, the interview will be conducted face-to-face at participants' locations. The questions will be asked directly.

In case of student, the questions will be sent via email to the participant. in the case of interviews, the questions will be asked as paper-based in written form at participants' locations.

2.4 External Institutions involved in the research (e.g. other university, hospital, prison etc.)

N/A

2.5 Name, telephone number, e-mail address and position of lead person for this project (plus full details of Project Supervisor if applicable)

1. Salam Ketab (Research student) - salam.ketab@plymouth.ac.uk, +441752586287
2. Prof. Nathan Clarke (Director of study) - N.Clarke@plymouth.ac.uk, +441752586226
3. Dr. Paul Dowland (Second Supervisor) - P.Dowland@plymouth.ac.uk, +441752586226

2.6 Start and end date for research for which ethical clearance is sought (NB maximum period is 3 years)

Start date: July 2016 **End date: December 2016**

2.7 Has this same project received ethical approval from another Ethics Committee?

No ☑ **Yes** ☐

2.8 If yes, do you want Chairman's action?

No ☑ **Yes** ☐

If yes, please include other application and approval letter and STOP HERE. If no, please continue

6. PROCEDURE

3.1 Describe procedures that participants will engage in, Please do not use jargon

Experts:

- At least 6 experts that have experience and qualification related to the research project will be identified.
- All the identified experts will be formally invited either in person or via e-mail.
- Once an expert initially accepted the invitation and prior to the interview, the consent form will be signed by the interviewee.
- A summary of how the system works including screenshots of the interfaces will be also emailed to the expert prior to the Interview.
- They will be then asked to suggest the time of conducting the interview.
- At the beginning of the interview, a demo of the system will be presented to the interviewee (about 20 minutes) in order to provide them with a better insight about how it works.
- A series of open-ended questions will be asked.
- All sessions will be recorded after having a permission of the interviewees, and transcribed afterwards. All interviews will be conducted in English to avoid translation bias. Finally, a copy of transcribed interviews will be send to academics confirming that they have been represented fairly and nothing critical missed in terms of the context or spirit of what they said.

Academics:

- At least 10 academics that have experience in university lecturing will be identified.
- All the identified academics will be formally invited either in person or via e-mail.
- Once an academic initially accepted the invitation and prior to the interview, the consent form will be signed by the interviewees.
- A summary of how the system works including screenshots of the interfaces will be also emailed to the academic prior to the Interview.
- They will be then asked to suggest the time of conducting the interview.
- At the beginning of the interview, a demo of the system will be presented to the interviewee (about 15 minutes) in order to provide them with a better insight about how it works.
- A series of open-ended questions will be asked.
- All sessions will be recorded after having a permission of the interviewees, and transcribed afterwards. All interviews will be conducted in English to avoid translation bias. Finally, a copy of transcribed interviews will be send to academics confirming that they have been represented fairly and nothing critical missed in terms of the context or spirit of what they said.

Students:

- At least 20 students will be formally invited either in person or via e-mail.
- Once they initially accepted the invitation, the students say they agree to participate by sending an email.
- A summary of how the system works including screenshots of the interfaces will be also emailed to the student (PowerPoint slides of the system to provide them with a better insight about how it works).
- In order to get their feedback, a set of questions will be sent to them via e-mail.

3.2 How long will the procedures take? Give details

The total amount of time needed for each expert participant will range between 30 to 35

minutes depending on the questions and the discussion. The total amount of time needed for each academic participant will range between 30 to 35 minutes depending on the questions and the discussion. The student participant will need about 25 minutes to see a demo of how the system works and then answer the questions.
3.3 Does your research involve deception?
No ☑ **Yes** ☐
3.4 If yes, please explain why the following conditions apply to your research: N/A
a) Deception is completely unavoidable if the purpose of the research is to be met
N/A
b) The research objective has strong scientific merit
N/A
c) Any potential harm arising from the proposed deception can be effectively neutralised or reversed by the proposed debriefing procedures (see section below)
N/A
3.5 Describe how you will debrief your participants
Prior to the interview, details of the research and proposed system including a demo of the system will be provided to the expert. They will be asked to read and understand all information to take part in the evaluation. Then a series of open-ended questions will be asked. All session will be recorded after having a permission of the interviewees, and transcribed afterwards. They are free to withdraw from the research at any stage, and ask for data to be destroyed if they wish at any time. Prior to the interview, details of the research and proposed system including a demo of the system will be provided to the academic. They will be asked to read and understand all information to take part in the evaluation. Then a series of open-ended questions will be asked. All session will be recorded after having a permission of the interviewees, and transcribed afterwards. They are free to withdraw from the research at any stage, and ask for data to be destroyed if they wish at any time. Prior to the questionnaire, details of the research and proposed system including a demo of the system will be provided to the students. All students will be asked to read and understand all information to take part in the evaluation. In order to get their feedback, a set of questions will be sent to them via e-mail. They are free to withdraw from the research at any stage, and ask for data to be destroyed if they wish at any time.
3.6 Are there any ethical issues (e.g. sensitive material)?

No ☑	**Yes** ☐
3.7 If yes, please explain. You may be asked to provide ethically sensitive material. See also section 11	
N/A	

4. BREAKDOWN OF PARTICIPANTS

4.1 Summary of participants

Type of participant	*Number of participants*
Non-vulnerable Adults	***Approximately 36***
Minors (< 16 years)	***N/A***
Minors (16-18 years)	***N/A***
Vulnerable Participants *(other than by virtue of being a minor)*	***N/A***
Other (please specify)	***N/A***
TOTAL	***Minimum 36***

4.2 How were the sample sizes determined?
The participants will be: • 6 experts in e-assessments, e-learning, or distance-based learning are considered a sufficient baseline to have obtain the necessary perspectives from research and practitioner based experts. • 10 university academics (e.g. PhD researches or staff members). • 20 undergraduate or postgraduate university students.
4.3 How will subjects be recruited?

- The experts will be recruited from inside or outside Plymouth University. They will be invited in person, via e-mail and/or professional social networks such as LinkedIn and Research gate, predominantly targeting people with experience and knowledge background in different areas. These areas are e-assessments, e-learning, and distance-based learning.
- The academics will be recruited from inside Plymouth University. Thy will be recruited in person or via e-mail, predominantly targeting people with experience and knowledge background in different areas.
- The students will be recruited from inside or outside Plymouth University. The will be recruited in person or via e-mail.

4.4 Will subjects be financially rewarded? If yes, please give details.

No

5. NON-VULNERABLE ADULTS

5.1 Are some or all of the participants non-vulnerable adults?

No ☐ **Yes** ✓ ☐

5.2 Inclusion / exclusion criteria

Participants who are 18 years old and above, agree and understand all procedure able to take part in this study.

5.3 How will participants give informed consent?

The participants will be given the consent at the beginning of the study, should they wish to carry out the study, ensuring their understand that they can withdraw from the study at any time up until the end of their participation. Please note that there is no possibility of involving any participant below 18 years old.

5.4 Consent form(s) attached

No ☐ **Yes** ☑

If no, why not?

N/A

5.5 Information sheet(s) attached

No ☐ **Yes** ☐ ✓

If no, why not?

N/A

5.6 How will participants be made aware of their right to withdraw at any time?
The right for participant to withdraw (at any time during the interview session or information/feedback collection process) is stated in the consent form.
5.7 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?
The recording of all participants' feedback will not contain any identifying information. With regards to the confidentiality, none of the results reported from the evaluation will include information that allows identification of named individuals.

6. MINORS <16 YEARS

6.1 Are some or all of the participants under the age of 16?		
No ☑		**Yes** ☐
If yes, please consult special guidelines for working with minors. If no, please continue.		

6.2 Age range(s) of minors		
N/A		
6.3 Inclusion / exclusion criteria		
N/A		
6.4 How will minors give informed consent? Please tick appropriate box and explain (See guidelines)		
N/A	**Opt-in** ☐	**Opt-out** ☐
6.5 Consent form(s) for minor attached		
N/A	**No** ☐	**Yes** ☐
If no, why not?		
N/A		
6.6 Information sheet(s) for minor attached		
N/A	**No** ☐	**Yes** ☐
If no, why not?		

N/A
6.7 Consent form(s) for parent / legal guardian attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
6.8 Information sheet(s) for parent / legal guardian attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
6.9 How will minors be made aware of their right to withdraw at any time?
N/A
6.10 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?
N/A

7. MINORS 16-18 YEARS OLD

7.1 Are some or all of the participants between the ages of 16 and 18?
No ☑ **Yes** ☐
If yes, please consult special guidelines for working with minors. If no, please continue.
7.2 Inclusion / exclusion criteria
N/A
7.3 How will minors give informed consent? (See guidelines)
N/A
7.4 Consent form(s) for minor attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A

7.5 Information sheet(s) for minor attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
7.6 Consent form(s) for parent / legal guardian attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
7.7 Information sheet(s) for parent / legal guardian attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
7.8 How will minors be made aware of their right to withdraw at any time?
N/A
7.9 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?
N/A

8. VULNERABLE GROUPS

8.1 Are some or all of the participants vulnerable? (See guidelines)
No ☑ **Yes** ☐
If yes, please consult special guidelines for working with vulnerable groups. If no, please continue.
8.2 Describe vulnerability (apart from possibly being a minor)
N/A
8.3 Inclusion / exclusion criteria
N/A

8.4 How will participants give informed consent?
N/A
8.5 Consent form(s) for vulnerable person attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
8.6 Information sheet(s) for vulnerable person attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
8.7 Consent form(s) for parent / legal guardian attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
8.8 Information sheet(s) for parent / legal guardian attached
N/A **No** ☐ **Yes** ☐
If no, why not?
N/A
8.9 How will participants be made aware of their right to withdraw at any time?
N/A
8.10 How will confidentiality be maintained, including archiving / destruction of primary data where appropriate, and how will the security of the data be maintained?
N/A

9. EXTERNAL CLEARANCES

Investigators working with children and vulnerable adults legally require clearance from the Disclosure and Barring Service (DBS)

9.1 Do ALL experimenters in contact with children and vulnerable adults have <u>current</u> DBS clearance? Please include photocopies.
No ☐ Yes ☐ N/A ☑
If no, explain
N/A
9.2 If your research involves external institutions (school, social service, prison, hospital etc) please provide cover letter(s) from institutional heads permitting you to carry out research on their clients, and where applicable, on their site(s). Are these included?
No ☐ Yes ☐ N/A ☑
If not, why not?

10. PHYSICAL RISK ASSESSMENT

10.1 Will participants be at risk of physical harm (e.g. from electrodes, other equipment)? (See guidelines)
No ☑ Yes ☐
10.2 If yes, please describe
N/A
10.3 What measures have been taken to minimise risk? Include risk assessment proformas.
N/A
10.4 How will you handle participants who appear to have been harmed?
N/A

12. PSYCHOLOGICAL RISK ASSESSMENT

11.1 Will participants be at risk of psychological harm (e.g. viewing explicit or emotionally sensitive material, being stressed, recounting traumatic events)? (See guidelines)
No ☑ Yes ☐
11.2 If yes, please describe
N/A
11.3 What measures have been taken to minimise risk?

N/A
11.4 How will you handle participants who appear to have been harmed?
N/A

12. RESEARCH OVER THE INTERNET

12.1 Will research be carried out over the internet?
No ☐ **Yes** ☑
12.2 If yes, please explain protocol in detail, explaining how informed consent will be given, right to withdraw maintained, and confidentiality maintained. Give details of how you will guard against abuse by participants or others (see guidelines)
Participants will be asked to confirm their age (must be at least 18 years old), understand that they can withdraw from the session at any time, and agree to participate in this evaluation by signing the consent form. The record kept of the expert feedbacks/outputs will not contain any identifying information about participants. With regards to the confidentiality, none of the results reported from this evaluation will include information that allows identification of the participants. All information will be treated as confidential at all times.

16. CONFLICTS OF INTEREST & THIRD PARTY INTERESTS

13.1 Do any of the experimenters have a conflict of interest? (See guidelines)
No ☑ **Yes** ☐
13.2 If yes, please describe
N/A
13.3 Are there any third parties involved? (See guidelines)
No ☑ **Yes** ☐
13.4 If yes, please describe
N/A
13.5 Do any of the third parties have a conflict of interest?
No ☑ **Yes** ☐
13.6 If yes, please describe

N/A

17. ADDITIONAL INFORMATION

14.1 [Optional] Give details of any professional bodies whose ethical policies apply to this research
N/A
14.2 [Optional] Please give any additional information that you wish to be considered in this application
N/A

18. ETHICAL PROTOCOL & DECLARATION

To the best of our knowledge and belief, this research conforms to the ethical principles laid down by the University of Plymouth and by any professional body specified in section 14 above.

This research conforms to the University's Ethical Principles for Research Involving Human Participants with regard to openness and honesty, protection from harm, right to withdraw, debriefing, confidentiality, and informed consent

Sign below where appropriate:
STAFF / RESEARCH POSTGRADUATES

	Print Name	**Signature**	**Date**
Principal Investigator:	Salam Ketab	_____	12/07/2016
	Prof. Nathan Clarke	_____	12/07/2016
	Dr. Paul Dowland	_____	12/07/2016

Staff and Research Postgraduates should email the completed and signed copy of this form to Paula Simson.

UG Students

	Print Name	**Signature**	**Date**
Student	_____	_____	_____
Supervisor / Advisor:	_____	_____	_____

Undergraduate students should pass on the completed and signed copy of this form to their School Representative on the Science and Environment Human Ethics Committee.

	Signature	**Date**
School Representative on Science and Environment Faculty Human Ethics Committee	_____	_____

Faculty of Science and Environment Research Ethics Committee List of School Representatives

School of Geography, Earth and Environmental Sciences	Dr Sanzidur Rahman
School of Biological Sciences	Dr Victor Kuri
School of Biomedical and Healthcare Sciences	Dr David J Price
School of Marine Science & Engineering	Dr Emily Beaumont (Chair)
	Dr Liz Hodgkinson
School of Computing & Mathematics	Mr Martin Beck
	Dr Mark Dixon
External Representative	Prof Linda La Velle
Lay Member	Rev. David Evans

Committee Secretary: Mrs Paula Simson
email: paula.simson@plymouth.ac.uk
tel: 01752 584503

SAMPLE SELF-CONSENT FORM
PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENVIRONMENT

Human Ethics Committee Sample Consent Form

CONSENT TO PARICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Salam Ketab

Title of Research

E-Invigilation of E-Assessments Syetem Evaluation

Brief statement of purpose of work

E-learning and particularly distance-based learning is becoming an increasingly important mechanism for education. Whilst a range of Virtual Learning Environments (VLEs) now exist to facilitate this, there are some significant limitations when considering the assessment options that are available. The lack of being able to provide invigilation in a remote-mode has restricted the types of assessments, with exams or in-class test assessments proving difficult to validate.

This study seeks to research and develop an e-invigilator that will provide continuous and transparent invigilation of the individual undertaking an electronic based exam or test.

Following the development of the system, to evaluate all dimensions of the E-Invigilation of E-Assessments system (EIEA), there are three separate stakeholder (namely: experts, academics and students) will get three separate sets of information and three separate sets of questions, in two cases it is a qualitative-based survey and the other one is a quantitative-based and qualitative-based survey.

- **Experts**: An expert-based (qualitative-based survey) evaluation will be taken place with the aim of validating the novelty, reviewing the performance and identifying its limitations.
- **Academics:** To prove the usability of the approach, the perspectives of the academics are also essential for additional qualitative evaluation (qualitative-based survey).

- **Student:** To prove the usability and non-intrusiveness of the approach, the student point of view is also necessary to add quantitative and qualitative evaluation.

You have the right to withdraw at any stage upon until the completion of the data collection process. Should you wish to withdraw from the study, please contact Salam Ketab.

For information regarding the study, please contact:

Salam Ketab – salam.ketab@plymouth.ac.uk

For any questions concerning the ethical status of this study, please contact the secretary of the Human Ethics Committee – paula.simson@plymouth.ac.uk

---

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations)

Under these circumstances, I agree to participate in the research.

Please select your group:

☐ Expert

☐ Academic

☐ Student

Name: ……..

Signature: .....…….. Date: .....……..

SAMPLE INFORMATION SHEET FOR ADULT / CHILD

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENVIRONMENT

RESEARCH INFORMATION SHEET

Name of Principal Investigator

Salam Ketab

Title of Research

E-Invigilation of E-Assessments Syetem Evaluation

Aim of research

The principle investigator has developed and implemented an e-invigilation of e-assessment prototype that will provide continuous and transparent invigilation of the individual undertaking an electronic based exam or test.

Description of procedure

For Experts:

All experts will be formally invited either in person or via e-mail. Once he/she initially accepted the invitation, prior to the interview, the consent form will be signed by the interviewees. A summary of how the system works including screenshots of the interfaces will be also emailed to the expert prior to the Interview. The expert will be then asked to suggest the time of conducting the interview.

All the session will be recorded (i.e. recording the entire Skype interview using special recording software) after having a permission of the interviewee and transcribed afterwards. The record will be destroyed (i.e. erased) after transcription. All interviews will be conducted in English to avoid translation bias. The total amount of time needed for each expert participant will range between 30 to 35 minutes depending on the questions and the discussion.

For Academics:

All academics will be formally invited either in person or via e-mail. Once he/she initially accepted the invitation, prior to the interview, the consent form will be signed by the interviewees. A summary of how the system works including screenshots of the interfaces

will be also emailed to the academic prior to the Interview. The academic will be then asked to suggest the time of conducting the interview.

All the session will be recorded (i.e. recording the entire interview using mobile phone recording application) after having a permission of the interviewee and transcribed afterwards. The record will be destroyed (i.e. erased) after transcription. All interviews will be conducted in English to avoid translation bias. The total amount of time needed for each academic participant will range between 30 to 35 minutes depending on the questions and the discussion.

For Students:

All students will be formally invited either in person or via e-mail. Once student initially accepted the invitation, prior to the interview, the consent form will be signed by him/her. A summary of how the system works including screenshots of the interfaces will be also sent to the student. The student will need about 25 minutes to see a demo of how the system works and then answer the questions.

Description of risks

All of the information will be treated confidentially and data will be anonymous during the collection, storage and publication of research material.

Benefits of proposed research

The lack of being able to provide invigilation in a remote-mode has restricted the types of assessments, with exams or in-class test assessments proving difficult to validate. This research seeks to research and develop an e-invigilator that will provide continuous and transparent invigilation of the individual undertaking an electronic based exam or test.

Right to withdraw

You have the right to withdraw at any time during the interview session.

If you are dissatisfied with the way the research is conducted, please contact the principal investigator in the first instance: telephone number *[*01752 586287*]*. If you feel the problem has not been resolved please contact the secretary to the Faculty of Science and Environment Human Ethics Committee: Mrs Paula Simson 01752 584503.

Appendix B: Publications

A Robust E-Invigilation System Employing Multimodal Biometric Authentication

Salam S. Ketab, Nathan L. Clarke, and Paul S. Dowland, International Journal of Information and Education Technology, pp796-802, Vol. 7, No. 11, ISSN: 2010-3689, 2017

The Value of the Biometrics in Invigilated E-Assessments

SS. Ketab, NL. Clarke, PS. Dowland, Proceedings of the 8th annual International Conference on Education and New Learning Technologies, in Barcelona (Spain) on the 4-6 July, pp7648-7658, ISSN: 2340-1117, 2016

E-INVIGILATION OF E-ASSESSMENTS

SS. Ketab, NL. Clarke, PS. Dowland, Proceedings of 9th International Technology, Education and Development Conference, Madrid, Spain. 2-4 March, pp1582-1591, ISSN: 2340-1079, 2015